C O V E N T R Y
U N I V E R S I T Y

Faculty of Engineering, Environment, and Computing

School of Computing, Electronics, and Mathematics

MSc Cyber Security

7030 CEM –Cyber Security Individual Project

“Information Security Management System (ISMS) of HAYS Technology”

Author: AKM HASAN

SID: 9755484

Supervisor: Dr. Leon Smalov

Submitted in partial fulfilment of the requirements for the Degree of Master of Science in MSc Cyber Security

Academic Year: 2021/22

Declaration of Originality

I declare that this project is all my work and has not been copied in part or whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet etc.), has been acknowledged by citation within the main report to an item in the References or Bibliography lists. I also agree that an electronic copy of this project may be stored and used for the purposes of plagiarism prevention and detection.

Statement of copyright

Statement of ethical engagement

I declare that a proposal for this project has been submitted to the Coventry University ethics monitoring website (https://ethics.coventry.ac.uk/) and that the application number is listed below (Note: Projects without an ethical application number will be rejected for marking)

Signed: *AKM MOMINUL HASAN* Date: 29 Jul 2022

Please complete all fields.

First Name:	AKM
Last Name:	HASAN
Student ID number	9755484
Ethics Application Number	P136420
1st Supervisor Name	Dr. Leon Smalov
2nd Supervisor Name	Dr. Christo Panchev

This form must be completed, scanned and included with your project submission to Turnitin. Failure to append these declarations may result in your project being rejected for marking.

Abstract

Keywords: ISMS, Cyber, “Global Cyber and InfoSec Strategy”, ISMS Policy, Strategic Context, Design, Implementation, Operations, Enforcement, Goals, Achievement, Global, Regional, Software, Security Life Cycle.

This project was adopted from the point of view of the Cybersecurity and Information Security Management System (ISMS) at HAYs Technology; during the Research Project I applied **Two Research Methodologies** in order to evaluate existing practice and potential risks at Hays and those Methodology included in these reports, and they are **Primary** (research plan) **Methodology** and **Secondary** (research design plan and practical Implementation) **Methodology**. Elucidations can be found later in these reports.

Table of Contents

Acknowledgments

I would like to thank my professors Dr. Leon Smalov and Dr. Christo Panchev for guiding me with their valuable feedback. I would also like to thank my partner for her unconditional love and support which reinvigorated my MSc in Cyber Security and brought me to this point.

Alongside this, I am also grateful to my IT Production Services Director Simon Gerhardt at Hays Central Services IT, with whom I had valuable discussions that shed light on topics that helped me with my project based on real-world scenarios at Hays, and also, I am grateful for his permission to do this Research Project from Hays Central Services IT, which is Hays's Global position for the Cyber Security and Information Security, and IT Operational Headquarter for 33 countries at Hays.

1. Introduction:

This Research Project is conducting a series of security operations within Hays ISMS, including Cyber Security. These reports are being completed purely based on real-world scenarios, and on-going-operations and in conjunction with all security teams at Hays.

At the same time, this team (ISMS team) is Implementing Hays Global Cyber and InfoSec Strategy, which means, with the **Strategic Context**, the ISMS team will enforce its **Implementation Phase** in order to reshape and improve Hays Cyber and Information Security situation. All security teams' activities, findings, and remediations can be found later in these reports in Secondary Methodology and Annexes.

2. Scope:

This Research Project is focusing on conducting and completing research based on Hays Central Services IT, which is a Global Position for Hays 33 countries; therefore, the Hays ISMS department is utilising Hays Global Cyber and InfoSec Strategy, and also, provides Guidelines and Directions to all security teams to each region and country based on Hays's ISMS policy. *[This paragraph is a copy of my own work, which I uploaded on my GitHub profile, as it is in progress on GitHub, GitHub. 2022. GitHub - AkmHasan/-: This Research Project will focus to conduct and complete a research based on Hays technologies and its central IT department. It is a global position, as Hays has branches in 23 countries.. [online] Available at: <https://github.com/AkmHasan/-> [Accessed 31 July 2022].*

More practical elements can be found later in these reports (Annex B and C), because this research will be conducted from Hays Central Services IT, and this is the position like a central hub for Hays's Cyber and Information Security and Operations centre in order to keep fit Hays business forefront.

3. Background:

This Project focused on reviewing past practice, present threats, and vulnerability gaps in the Global IT security roles at Hays; therefore, the focal point is the Central Services IT department at Hays Global InfoSec Headquarter. This organisation maintains its Global Cyber and InfoSec Strategy, and this Global Strategy advice and direction to the ISMS Policy to follow the Global Strategy from the view of Strategic Context and advise to Implement those with other security policies, and also, it (Global Strategy) also, advice to the ISMS Policy that how the ISMS Policy should governance within the UK and worldwide, but the Central Services IT department is based in the UK and this Research Project is taking part in the UK headquarter, hence, this project must focus on the UK law, and legislation; alongside this, its previous and current assessment reports in order to maintain Hays ISMS functionality.

This Central Services IT department is a Global IT and Cyber Management position, and also this department approves policies for the other regions and branches; therefore, for this reporting purpose is mentioning about 3 branches of Hays but for the known commercial restrictions and company's ISMS policy and GDPR, readers should assume those regions as region **A** or **APAC** (it cover the whole Asia Pacific), region **E** or **EME/A** (it cover the whole Europe, Middle-Est and America), and region **U** or **UK&I** (it cover the whole UK and Ireland), and their activities, operational functions, and ISMS functions explained later on this report. For this Research purpose, we can assume that

Hays's Annual IT and Cyber budget is only **"£18 million"** for the UK&I, and for Global, it is **"£45 million"**.

A complete overview of Hays ISMS Capabilities, function, and full IT and Cyber structure is given below based on real-world IT and Cyber Operations and Implementation by Hays Cyber Security Manager (which is the Author of this Research Project), and the document extracted from Hays's Cyber Security Manager's Operational Diary and Strategic Roadmap for Hays Cyber and ISMS.

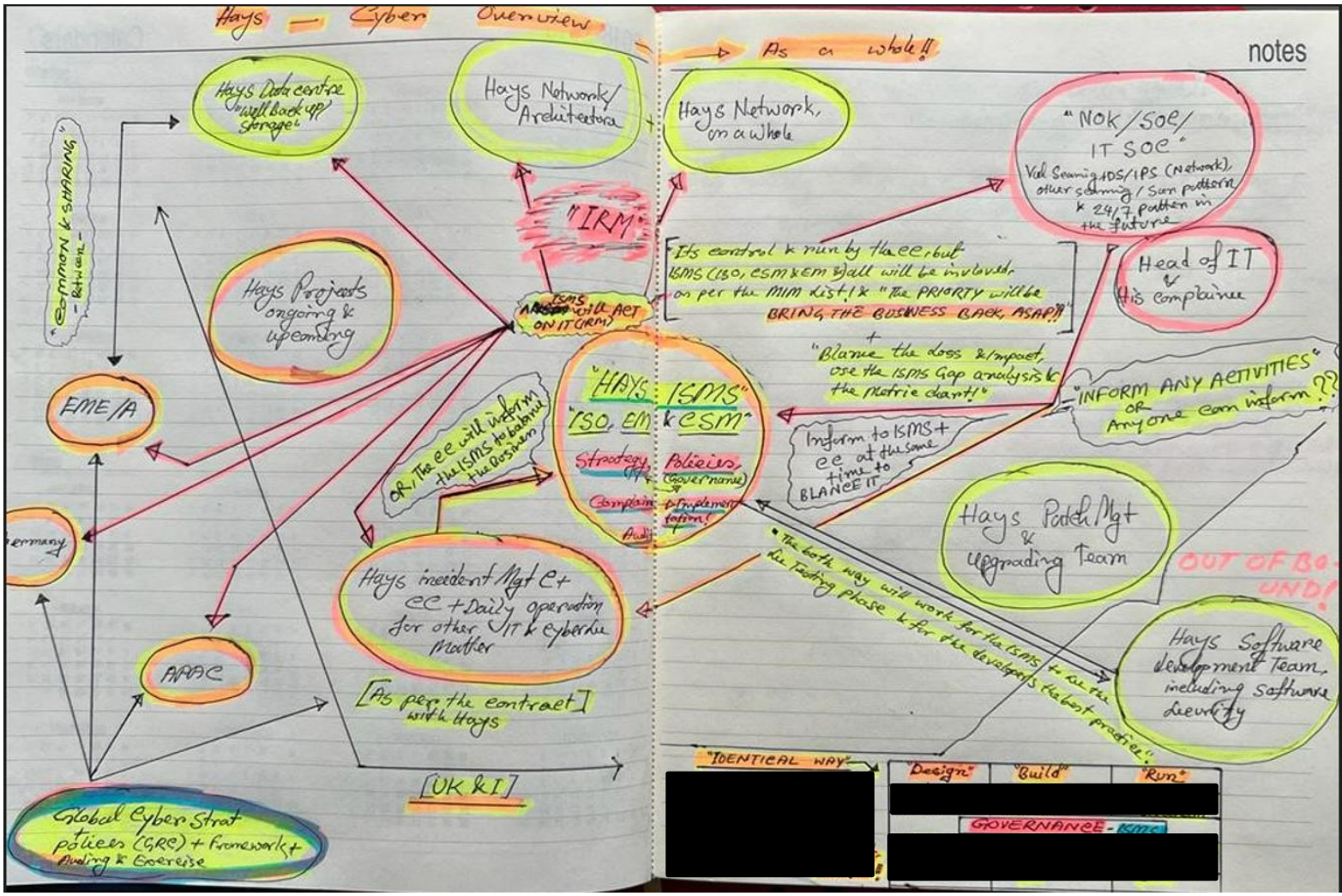


Figure: 01 – Hays IT and Cyber functioning Clockwise, this document is extracted from Hays's Cyber Security Manager's Operational diary and roadmap. Data has been hidden for GDPR purposes.

4. Aim and Objectives:

The main aim of this project is to identify threats and risks in Hays's Cyber and Information Security Management System (ISMS) boundaries, then evaluate them within the ISMS capabilities and if requires then assess with Hays Risk Matrix and in conjunction with other security teams (SOC, Hays's (Manage Service Provider) MSP Computacenter, Data centre, Patching team, Network team), and mitigate the risks for the organisation in order to carry out Hays's daily business.

Sometimes, requires (risk factors) to raise at Hays Global Cyber Committee meeting meetings in order to assess by the Global Risk Matrix at Hays.

To do this, this report is gathering all the incident reports and findings provided by Hays's Internal security team (SOC) and also, the external security team (A&O IT Group), if required then also will be gathering more evidence, which will be helping to do a proper evaluation of the Hays ISMS team.

Moreover, to gather these Data and reports, I will be collecting everything from Hays's different teams because currently Hays implementing the world's sophisticated tools provided world's Tech giant companies, i.e. Microsoft, Tenable, Splunk, RiskRecon, and sometimes 3rd party companies, i.e. NCC Group or A&O IT Group. However, all reports and their remediation actions will be explained in **Secondary Methodology** and **Annex A, B, and C** very end of this Research Project.

Additionally, with all software and its output, these reports will be using threat modelling procedure by Hays's SOC team, security life cycle (used by Hays's ISMS team), a gap assessment to understand how the matrix looks like, auditing, and a control-based approach for the organisation and will provide a development plan in order to mitigate those issues have found, and for the business continuation. Sometimes, Hays's ISMS team conducts an **Internal Auditing** process, and sometimes **External Auditing** is conducted by a 3rd party, i.e. **PWC** and **KPMG**. Details of these could be found later in **Annex A, B, and C** very end of this Research Project.

Furthermore, to evaluate these risks, Hays uses a simulation Phishing test, and this test is implemented in order to educate Hays's employees, and more detail can be found later in this report; similarly, Hays is Globally organising an Incident Response Management (IRM) process, and it's based on OWASP's top 10 vulnerabilities. This Research Project also focuses, on the whole Confidentiality, Integrity, and Availability (CIA) triage for its Conditional Access (CA) for Hays IT decorate in order to maintain its security functionality, and to this Hays added another extra layer for its security, which is Multi-Factor Authentication (MFA), this can be found later of this Research project.

To complete this Research Project will be utilising and including some live Data (as per company guidelines and its **CIA** policy) and its output from some sophisticated tools ay Hays, which are used in order to mitigate Cyber and Information risks, which directly could impact Hays ISMS and its Cyber Security, and Cyber Security is another main part or **sub-branch** of the ISMS at Hays.

Additionally, to complete this project will be implementing the Data, Information, and Incident Response Management Plan (as per company guidelines and its **CIA** policy) from Hays real-world **IRM** team (from Hays **U** and **A** – Acronym explained above in Background of this Project), which is always updating, conducting, and monitoring by Hays ISMS team.

To get a successful result at the end of this project, the considered risks must be assessed correctly; however, all theoretical and practical elements will be limited in this report because of the company policies but whatever will be provided will be based on real-world scenarios and current Operations within ISMS and Cyber Security (sub-branches of ISMS) at Hays Central Services IT. The specific limitations will be explicitly identified in the project report.

5. Primary Methodology for Hays ISMS Project:

5.1. Hays Global Cyber and InfoSec Strategy:

This report is identifying and evaluating the existing policy and Hays's brand new Global Strategy for Cyber and Information Security; therefore, have gone through most of the previous security policies for this organisation; however, there wasn't any firm Strategy for the global position earlier when this project proposal submitted, but recently Hays Global Cyber and InfoSec Strategy draft has completed by Hays's Cybersecurity Manager (who is the author of this Research Project), UK and provided this to Hays's Information Security Management System (ISMS) team at Hays central IT department, and this Global Strategy will be utilising all of the security related matters at Hays Global Cyber and InfoSec prospects, this Global Strategy will be used to evaluate this Research Project.

(Reference: Figures 02 and 03 illustrate more clarity about the Global Strategy, which was extracted from "Hays Global Cyber & InfoSec Strategy" main documents at Hays.)

This Global Strategy will go live from September 2022 for all Hays branches around the world in order to **Implement** and **Enforce** based on the Strategic Context, which **enables** all Managers in ISMS and Cyber departments at Hays (Globally).

5.2. Hays ISMS Policy:

Alongside this, the **Primary Methodology** of this project is mainly focusing on the **Strategic context** of the Information Security Management System (ISMS) of Hays Central Services IT. Additionally, this part defines Hays ISMS team and its **Sub - branches**, i.e. Cyber security Strategic Management, Security Operation Centre (**SOC**), and other regional security teams that come under Information Security or **ISMS** branch, later in this report can be found their (sub-branches) activities and function in order to secure Hays Data and Information in this Information Age.

Hence, the ISMS team of Hays provides an overview of Cyber and Information Security by using Hays Global Cyber and InfoSec Strategy, which is more practical and operational at Hays, rather than an inspirational type of Strategy. This Global Strategy directly **enable** Hays Information Security or ISMS policy and Security policies, i.e. Operation Centre (**SOC)** policy in order to carry out their function at Hays. However, more policies and Implementation parts can be found in the **Secondary Methodology** of this Research Project (a – **Conceptual Phase**, and b – **Practical Phase**).

Following the Global Strategy for assessing risks and threats from every dimension is collecting all current and previous information, reports, and findings related to Information Security, gathering all other data, and will be putting them together in order to get a perfect solution from its assessment.

To do this, most of the security teams are involved and providing their reports to evaluate and mitigate risks for Hays Information and Cyber security.

Reference - Hays Global Cyber and InfoSec Strategy is given below but the whole document could be found in **Appendix C** with a sequential explanation.

HAYS Working for your tomorrow

HAYS GLOBAL CYBER & INFOSEC STRATEGY

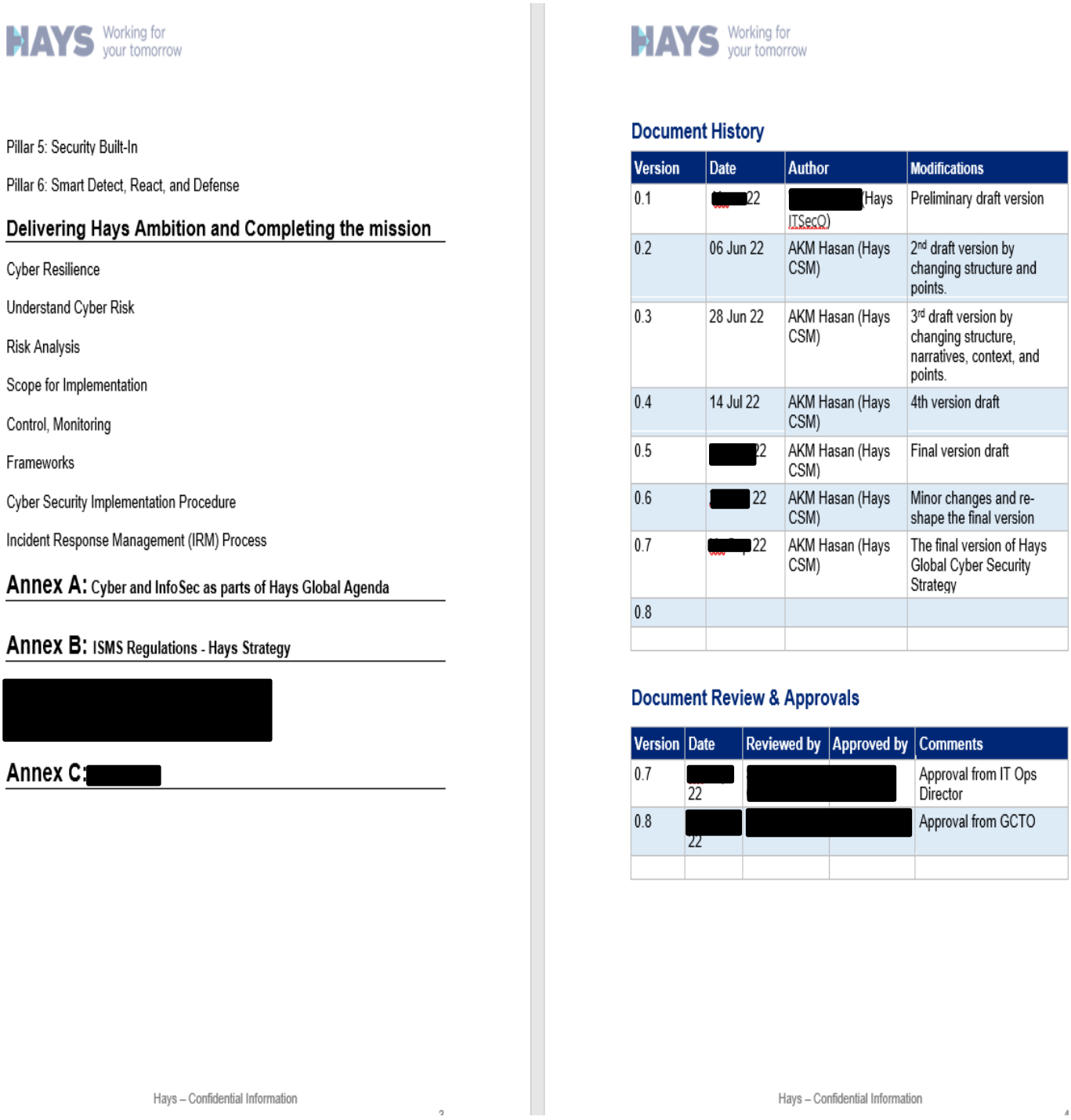
SECURING HAYS INFORMATION

HAYS Working for your tomorrow

CONTENTS

2

Figure: 02 -This document was extracted from Hays Global Cyber & InfoSec Strategy.



HAYS Working for your tomorrow

Pillar 5: Security Built-In

Pillar 6: Smart Detect, React, and Defense

Delivering Hays Ambition and Completing the mission

Cyber Resilience

Understand Cyber Risk

Risk Analysis

Scope for Implementation

Control, Monitoring

Frameworks

Cyber Security Implementation Procedure

Incident Response Management (IRM) Process

Annex A: Cyber and InfoSec as parts of Hays Global Agenda

Annex B: ISMS Regulations - Hays Strategy

[redacted]

Annex C: [redacted]

Hays – Confidential Information

HAYS Working for your tomorrow

Document History

Version	Date	Author	Modifications
0.1	[redacted]22	[redacted] (Hays ITSecO)	Preliminary draft version
0.2	06 Jun 22	AKM Hasan (Hays CSM)	2nd draft version by changing structure and points.
0.3	28 Jun 22	AKM Hasan (Hays CSM)	3rd draft version by changing structure, narratives, context, and points.
0.4	14 Jul 22	AKM Hasan (Hays CSM)	4th version draft
0.5	[redacted]22	AKM Hasan (Hays CSM)	Final version draft
0.6	[redacted]22	AKM Hasan (Hays CSM)	Minor changes and re-shape the final version
0.7	[redacted]22	AKM Hasan (Hays CSM)	The final version of Hays Global Cyber Security Strategy
0.8			

Document Review & Approvals

Version	Date	Reviewed by	Approved by	Comments
0.7	[redacted]22	[redacted]		Approval from IT Ops Director
0.8	[redacted]22	[redacted]		Approval from GCTO

Hays – Confidential Information

Figure: 03 – Figures 02 and 03 these documents were extracted from Hays Global Cyber and InfoSec Strategy main document, and the full documents could be found in **Annex C.**

Moreover, data is collected via an electronic mailing system (Email), Microsoft Team (MS Team), data mining, and other tools (software) available at Hays; additionally, I am conducting interviews with the relevant departments (relevant SME), and departmental heads to put a valuable impact and information to complete this Research Project based on current IT and Cyber activities at Hays Global scope.

The **Primary Methodology** of this Research Project will be giving a crystal-clear view to its readers about the **Strategy** and **Strategic Context**, as per Hays Global Cyber and InfoSec Strategy, but the **Secondary Methodology** of this Project will elucidate more about **Implementation Phase** and the **Global and Regional projects** of Hays ISMS will expand more about its **Ambition completing mission Phase**, which is how Hays enforce its ISMS Policy and other Information Security Policies and carry out ISMS's operations; maintain its function for Information Security to keep fit Hays business forefront.

Furthermore, Hays Cybersecurity Manager (**CSM**)and Information Security Officer (**ISO**) are ultimately responsible for "**Hays Global Cyber & InfoSec Strategy"** and the **Primary Methodology** of this Research Project is to explain more about it, as they comply with the Global Strategy from a very high level, and they push it down towards all security teams within Hays Globally and Regionally. This Strategy owned by the Group Chief Technical Officer (**GCTO**) at Hays and the IT Services Product Director has the overall visibility, but Hays's Cyber Security Manager (**CSM**) and Information Security Officer (**ISO**) are accountable to push it further at Hays for its Information and keep the momentum for the Cyber and Information security operations.

Alongside this, another focal point of this **Primary Methodology** is providing a roadmap for educating its employees; and is achieved by conducting interviews with all relevant team leaders and by gathering reports about their employee's strengths and knowledge about **Cyber** and **Information Security**. After a proper evaluation, Hays's Cyber Security Manager (**CSM**) and Information Security Officer (**ISO**) liaise with Hays IT Services Director and Hays's People and Culture team Hays P&C) in order to conduct the Training and Awareness for its employee in relation to the **Cyber** and **Information Security**. This Training and Awareness program lies with "**Hays Global Cyber and InfoSec Strategy**" and Hays's ISMS Policy; therefore, it pushes toward the Global and Regional facilities for its employees. Further details will be found in **Annex C** of this Research Project.

Similarly, for the Phishing simulation practice and Test for Hays's employees, if any employee clicks or hits the Phishing button or any Phishing email, then they must go through mandatory Phishing training provided by 3rd party organisation to Hays. Further details will be found in **Project Outcome** and in **Annex C**, at the very end of this Research Project.

The **Primary Methodology** not only explains the **Strategic Context** and **Scope** for Cyber and Information Security but also provides Hays's **vision**, **goals**, and **principles** in relation to Hays Cyber and IT security; alongside this, this methodology elucidates about Information team's **role**, **responsibilities**, and **authorities**. The magnificent part of this **Methodology** is this Phase (Primary Methodology) **introduces** and **enables** the **enforcement method** of each security role at Hays to **reshape** and **create** its Cyber and Information defense shield against attackers. More details can be found in **Secondary Methodology** and in **Annexes**, which are later in this Research Project.

However, those explanations are giving in **Secondary Methodology** and **Global projects** (all branches, **U**, **E**, and **A** - Acronym explained above in Background of this Project) are only for readers to understand the **Practical Phase** of Hays ISMS function and Information of Security (InfoSec) policy, but more details can be

found sequentially in **Annexes (Annex A, B,** and **C**) at the end of this Research Project.

The reader should understand that these are merely a few outputs from the whole Information Security function (ISMS) at Hays and these are utilising only for this Research project purpose, additionally, I can not add all of the Operational factors for this Research Project, as all data and information is confidential and I am not allowed to provide most of these due to its commercial purpose, policy restriction, and GDPR.

6. Secondary Methodology for Hays ISMS:

There are two types of areas that are covered in this report, those are below:

a) Conceptual and **b)** Practical

However, both areas and their function are described based on “Hays Global Cyber and InfoSec Strategy” and ISMS Policy, and any other policies, which lies within the ISMS policies (sub-branches).

6.1. Conceptual:

6.1.1. Hays ISMS Lifecycle:

The Conceptual part of the **Secondary Methodology** is the **Design Phase** for this Research Project that will be following the **Information Security Life Cycle** and its goals at Hays in order to complete this assessment.

(Reference: Figure 04 illustrates more clarity about the Information Security Life Cycle, which was extracted from the “7033 CEM module at Coventry University” in order to evaluate Hays’s ISMS function at Hays and this Research Project.)

The **Conceptual Methodology** mainly describes more about Hays's Information Security Management System (ISMS) policy and its roadmap. “Hays Global Cyber and InfoSec Strategy” is a very high-level document that provides the vision, and directions to the ISMS Policy that should drive Hays Information Security Management System to achieve its goals. A lot of branches are under Hays’s ISMS branch, which we have known as sub-branches of Hays ISMS and this (ISMS) Security Policy provides Guidelines and Directions (**G&D**) to its (Hays) security teams, employees, and also, who are related to its business, and 3rd party contractors.

However, this Methodology always follows and Implements the Security Lifecycle based on Hays ISMS goals. See the ISMS Security Lifecycle below:

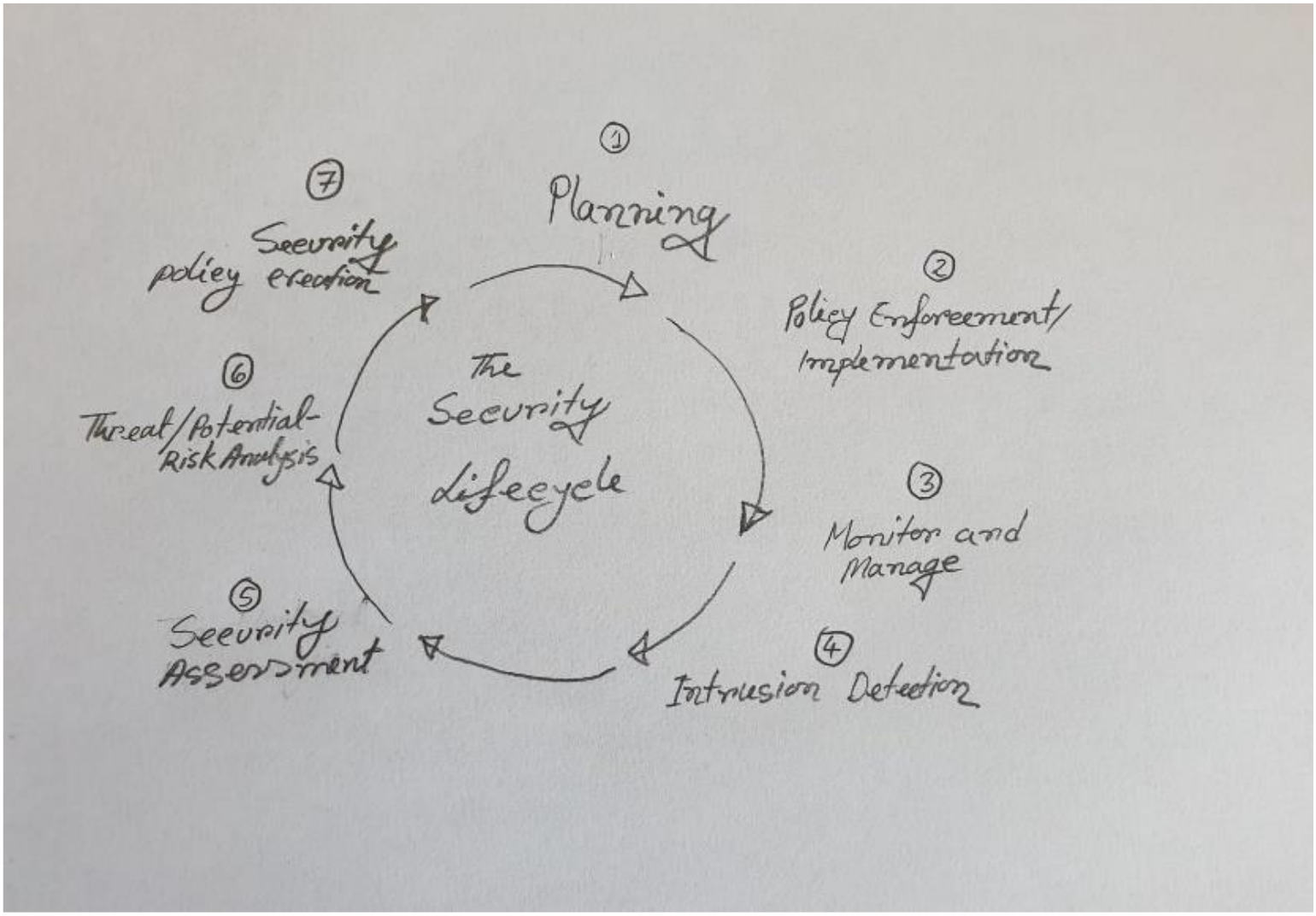


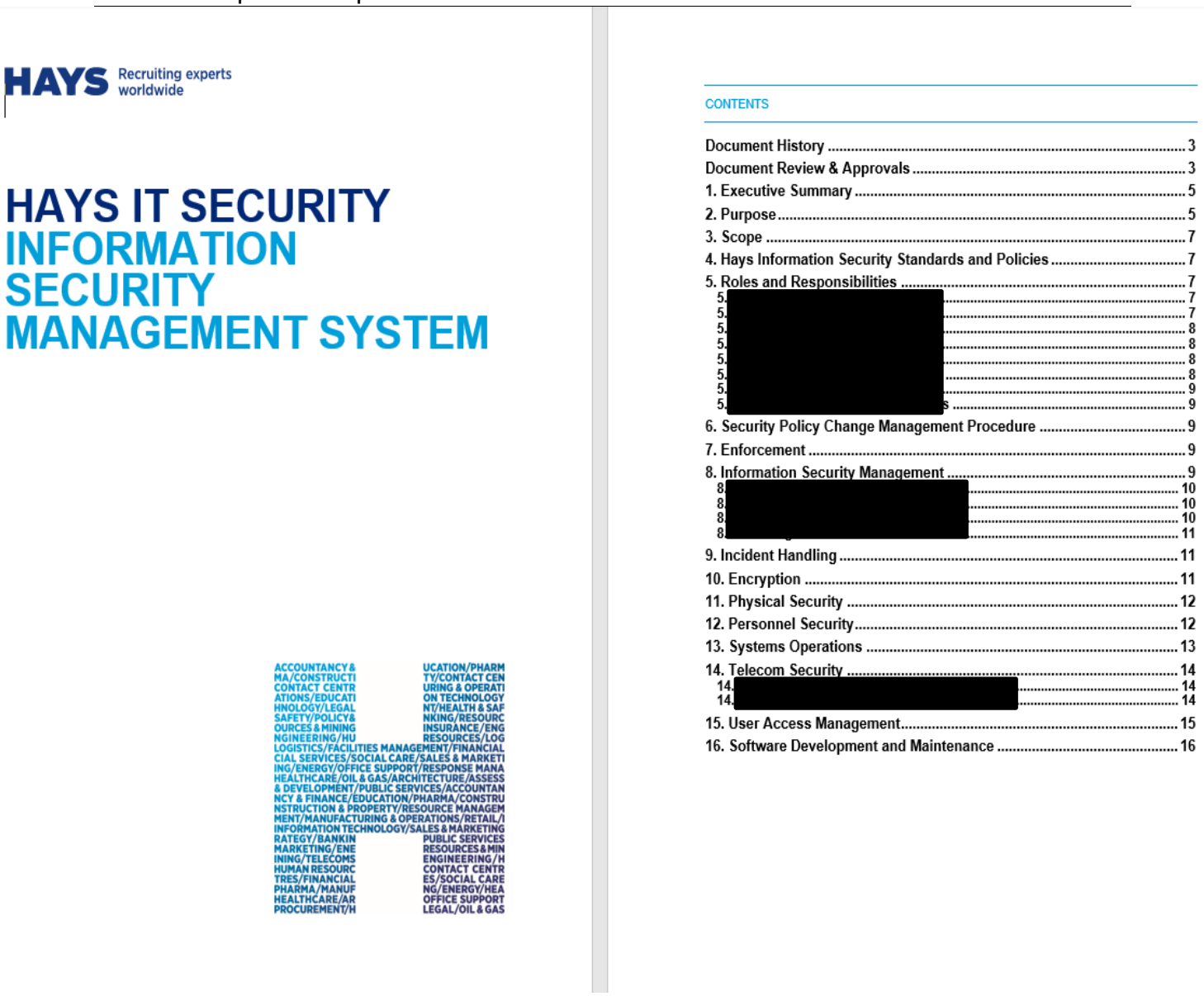
Figure: 04: ***Reference*** - This diagram I have taken from my own module and own drowning at **Coventry University** with Dr. Leon Smalov, which was **7033CEM** – "Information Security Risk Assessment for ABC Air" and submitted the last term.

This Methodology is aiming to explain to Hays employees how important security areas are at Hays, and its employees should and must act on it in relation to Information and Cyber Security, as per ISMS policy. This policy captured pretty much every section for Hays Information Security and its implementation and for the best practice at Hays.

(Reference: Figure 05 illustrates more clarity about the Information Security Management System Policy, which was extracted from "Hays ISMS Policy" main documents at Hays.)

Alongside this, the ISMS policy **enables** all security managers' **authority** and **enforcement** to do **Internal Auditing** and arrange any **External Auditing** process. This Methodology not only provides the Guidelines and Direction (**G&D**) but also included that if any employee fails to comply with the ISMS Policy and will face disciplinary action, the consequences could be a possible dismissal.

Hays ISMS Policy is given below but the whole document could be found in **Appendix C** with a sequential explanation.



HAYS Recruiting experts worldwide

HAYS IT SECURITY INFORMATION SECURITY MANAGEMENT SYSTEM

ACCOUNTANCY & UCATION/PHARM
MA/CONSTRUCTI TY/CONTACT CEN
CONTACT CENTR URING & OPERATI
ATIONS/EDUCATI ON TECHNOLOGY
HNOLOGY/LEGAL NT/HEALTH & SAF
SAFETY/POLICY& NKING/RESOURC
OURCES & MINING INSURANCE/ENG
NGINEERING/HU RESOURCES/LOG
LOGISTICS/FACILITIES MANAGEMENT/FINANCIAL
CIAL SERVICES/SOCIAL CARE/SALES & MARKETI
ING/ENERGY/OFFICE SUPPORT/RESPONSE MANA
HEALTHCARE/OIL & GAS/ARCHITECTURE/ASSESS
& DEVELOPMENT/PUBLIC SERVICES/ACCOUNTAN
NCY & FINANCE/EDUCATION/PHARMA/CONSTRU
NSTRUCTION & PROPERTY/RESOURCE MANAGEM
MENT/MANUFACTURING & OPERATIONS/RETAIL/I
INFORMATION TECHNOLOGY/SALES & MARKETING
RATEGY/BANKIN PUBLIC SERVICES
MARKETING/ENE RESOURCES & MIN
INING/TELECOMS ENGINEERING/H
HUMAN RESOURC CONTACT CENTR
TRES/FINANCIAL ES/SOCIAL CARE
PHARMA/MANUF NG/ENERGY/HEA
HEALTHCARE/AR OFFICE SUPPORT
PROCUREMENT/H LEGAL/OIL & GAS

CONTENTS

Figure: 05 - This document was extracted from Hays ISMS Policy main document, and the full documents could be found in **Annex C.**

This ISMS Policy lies with the Security Operation Centre (**SOC**) Policy, as mentioned at the top that Hays ISMS has sub-branches, and the **SOC** is one of them. The Security Operation Centre or **SOC** is the Eye of **Hays Central Services IT** and **Group IT Services**, and it covers the front-line defense for Hays, and also, performs as a Network Operation Centre (**NOC**).

(Reference: Figure 06 illustrates more clarity about the Security Operation Centre (SOC), which was extracted from "Hays SOC Policy" main documents at Hays.)

However, "Hays Global Cyber and InfoSec Strategy" and its ISMS Policy advise and provides Guidelines to the **SOC** that how the **SOC** should and must operate and carry out its functions in order to keep Hays's network and

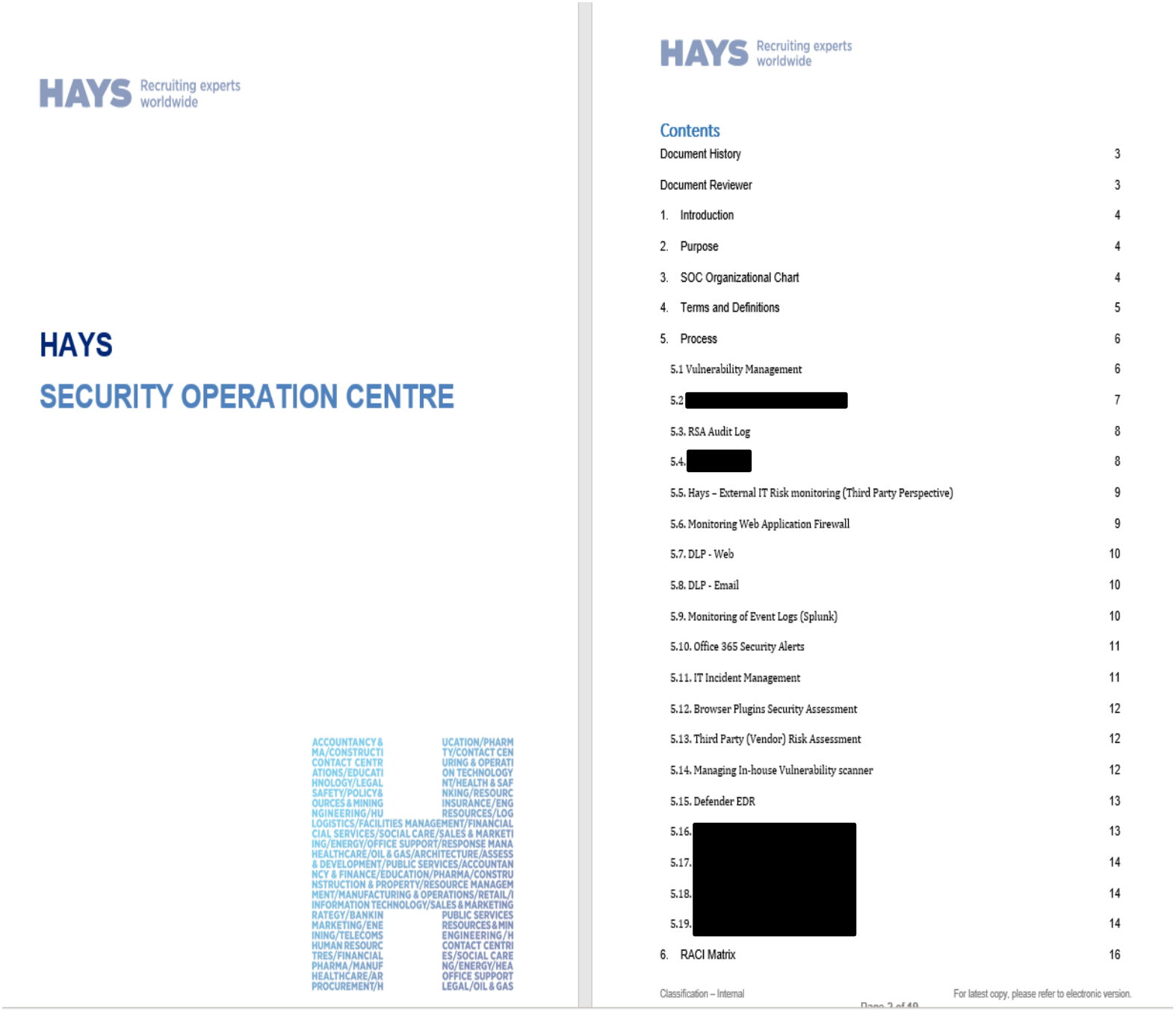
systems safe from any potential data breach or any kind of attacks whether it is an insider or outsider threat.

To do these tasks based on all policies, the **SOC** is using the world's sophisticated tools, i.e. **Splunk**, **Microsoft Defender (MS. D)**, etc. The elucidation about these can be found in this Methodology in the **Practical** part.

At the same time, the **SOC** establishes communication with Hays Manage Service Provider (**MSP**) Computacenter (**CC**) for Hays Data centre (**DC**) in Romford and Manchester, UK. By doing these the Security Operation Centre (**SOC**) create ongoing channels that collaborate and share all Data and Information in order to keep Hays's network, system, and valuable assets safe and secure, and if any abnormality or suspicious activities they (**SOC**) find then the **SOC** raise it with Hays Cyber Security Manager and Hays ISMS team in order to evaluate them and for the best advice to mitigate them.

The **Conceptual** part of this Research project provides better clarity and a pen-picture of the **Practical part** of the **Secondary Methodology** and how the Global Strategy and ISMS Policy reflect Hays's Information Security Life Cycle. Moreover, the Conceptual part provides an indication for Hays Global and Regional projects of ISMS in conjunction with the Security Operation Centre (**SOC**), Computacenter (**CC**), Data Centre (**DC**), and Hays ISMS team at Hays Central Services IT; these teams (especially, the ISMS team) controls Global projects and pushes down to regional branches to achieve them within its set timeline.

Hays Security Operation Centre (SOC) Policy is given below but the whole document could be found in **Appendix C** with a sequential explanation.



HAYS Recruiting experts worldwide

HAYS

SECURITY OPERATION CENTRE

ACCOUNTANCY & UCATION/PHARM
MA/CONSTRUCTI TY/CONTACT CEN
CONTACT CENTR URING & OPERATI
ATIONS/EDUCATI ON TECHNOLOGY
HNOLOGY/LEGAL NT/HEALTH & SAF
SAFETY/POLICY& NKING/RESOURC
OURCES & MINING INSURANCE/ENG
NGINEERING/HU RESOURCES/LOG
LOGISTICS/FACILITIES MANAGEMENT/FINANCIAL
CIAL SERVICES/SOCIAL CARE/SALES & MARKETI
ING/ENERGY/OFFICE SUPPORT/RESPONSE MANA
HEALTHCARE/OIL & GAS/ARCHITECTURE/ASSESS
& DEVELOPMENT/PUBLIC SERVICES/ACCOUNTAN
NCY & FINANCE/EDUCATION/PHARMA/CONSTRU
NSTRUCTION & PROPERTY/RESOURCE MANAGEM
MENT/MANUFACTURING & OPERATIONS/RETAIL/I
INFORMATION TECHNOLOGY/SALES & MARKETING
RATEGY/BANKIN PUBLIC SERVICES
MARKETING/ENE RESOURCES & MIN
INING/TELECOMS ENGINEERING/H
HUMAN RESOURC CONTACT CENTRI
TRES/FINANCIAL ES/SOCIAL CARE
PHARMA/MANUF NG/ENERGY/HEA
HEALTHCARE/AR OFFICE SUPPORT
PROCUREMENT/H LEGAL/OIL & GAS

HAYS Recruiting experts worldwide

Contents

Classification – Internal For latest copy, please refer to electronic version.

Figure: 06 - This document was extracted from Hays SOC Policy, and the full documents could be found in **Annex C.**

6.2. Practical:

The practical part of this Research Project is the **Project's Testing part** or **Testing Phase**, which will be going through most of the **practical** and **operational** parts at Hays within the Information Security Management System (ISMS) capability (*within the scope for this project due to its commercial policy restriction and GDPR*), and these parts **Implementing** the **Security Lifecycle** based on "Hays Global Cyber & InfoSec Strategy" and ISMS Policy. All those areas of Operations and Implementations will be explained in the **Secondary Methodology** of this Research Project, but all those supplements and more details will be provided in **Annexes** very end of this project.

However, only one practical part will be running by simulation method to complete for this Research Project at Hays, as this report will simulate potentially dangerous things, and assess and mitigate the risks like other operational factors indicated above.

Furthermore, all **practical activities** are presented for this Research Project based on the Information Security Management System (ISMS) and Cyber overview at Hays, and this project is identifying that Hays's ISMS team maintaining the momentum of its **Governance**, **Methodology,** and **Operations** in order to complete all practical Phase sequentially in order to secure Hays Data and Information.

Everything elucidates *sequentially* below, including **Global and Regional Projects** conducted by Hays ISMS and Cyber teams.

To complete the **practical parts** of this Research Project, the practical parts are further focusing on some sophisticated tools and their functionalities at Hays to collect Data and Information and to evaluate this project, and those tools are, Microsoft Defender (**MS. D - EDR solution**), Browsing Plug-in Security Assessments (**Plug-In SA**), Splunk (Pro-Active monitoring of Hays's Asset), Web – Application Firewall monitoring (**WAF**), **3rd Party Risk Advisory** (for EMEA), **365 Office** (Security Monitoring).

Recently, Hays spent around **"£7 million"** (for each year license cost) for the **Microsoft E 5 Licence** for its Global solution for its (Hays) business and C-Suite security, and spent **£0.5 million** for **Tenable SC** (Nessus) Global Software (for Vulnerability Scanning) and Hays Implementing the Global Incident Response Management (**IRM**) process, based on new Information law as of effect 28 April 2022 sets by the Government of India; by Implementing all these **3 Global processes** all Data and Information related matter is becoming centralisation at Hays Central Services IT and coming under one umbrella for its Global Controls and Operations as per "Hays Global Cyber and InfoSec Strategy".

*(**Reference** – Figure 07 illustrates more clarity about the new law sets by the Government of India, which was extracted from Technology Law Advisory – CRET Regulation, 2022 main document.)*

Additionally, all are described below for the **U** (**Global position**), **E**, and **A** region - Acronym explained above in the "***Background part***" of this Project (**Practical Phase**):

KOCHHAR & CO.
ADVOCATES & LEGAL CONSULTANTS

Technology Law Advisory – CERT Regulations, 2022

INTRODUCTION

On April 28, 2022, the Indian Computer Emergency Response Team ("CERT") which is part of the Ministry of Electronics and Information Technology issued directions ("Direction") under Section 70B of the Information Technology Act, 2000 relating to reporting of cyber security incidents. This client update summarizes the requirement under the law and analyses the implications of the same.

BACKGROUND

The CERT was set up some years back to function as the nodal agency in the area of cyber security. It's powers include the collection, analysis and dissemination of information on cyber security incidents, providing forecasts and alerts, taking emergency measures and co-ordination of responses to cyber security incidents. It also has powers to issue directions to "service providers, intermediaries, data centres, and body corporates". Thereafter, certain rules were issued relating to CERT which also covered breach notification requirements. The rules were ambiguously worded and did not make clear that such notifications were mandatory. It related to cyber security incidents generally and was not related to breach of personal information of Indian citizens. Further, it did not address incidents that involved Indian businesses but where the concerned server was located outside India. It has therefore been a challenge to determine to what extent breach notifications were required in the case of global incidents with implications to Indian businesses.

Figure: 07 – *The new law sets by the Government of India. This document was extracted from Technology Law Advisory – CRET Regulation, 2022 main document, but the full documents could be found in* ***Annex C****.*

6.2.1. Microsoft Defender (MS. D) for the UK&I:

Function - Microsoft Defender (MS. D) is End Point Detection and Response (EDR) solution for Hays. This EDR solution has changed the previous Anti-Virus at Hays systems and established a new security layer at Hays.

MS. D is able to carry out Vulnerability Assessments at Hays systems on a regular basis, it's monitoring Software's End of Lifecycle (EOL) as well. This EDR solution is managed by the Hays (MSP) Computacenter (CC) for the UK and Ireland only (UK&I); however, the Security Operation Centre (SOC) maintains the Governance for other regions (EMEA and APAC), and their (regional) security teams are responsible to manage MS. D EDR.

Implementation - The EDR solution activities (**Practical Phase**) are provided in order to understand its readers how its reports generate and how its managed by CC (for the UK&I) and Governance by the SOC (for other regions), and how the ISMS team act on those for Hays IT and Cyber Operations and Implementation. However, the documents below only give you an idea that how **MS. D EDR** performs but the whole Practical documents can be found in **Annex C** end of this Research Project.

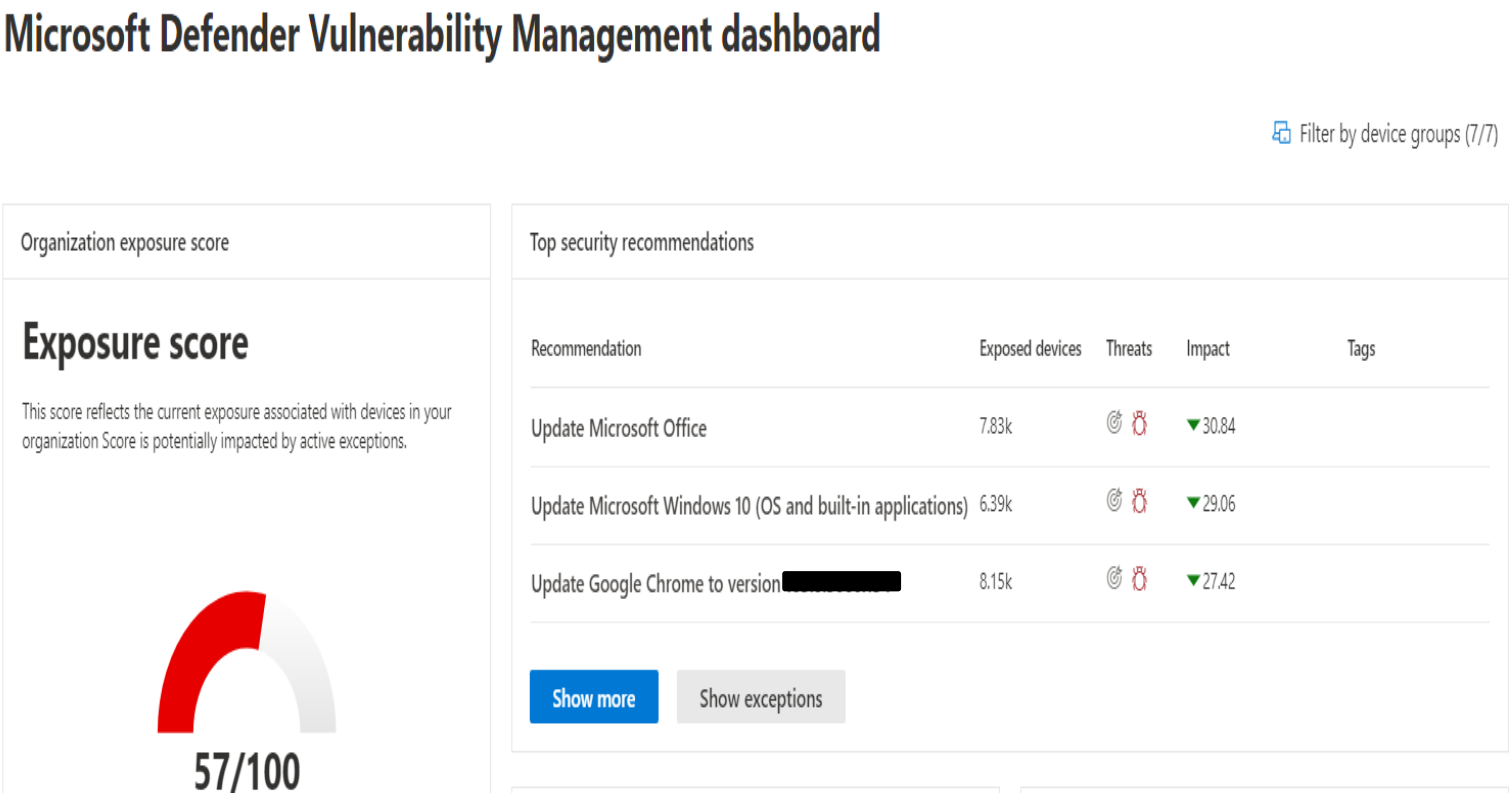


Figure: 08 - Microsoft Defender reports, on how to monitor **EOL**, Vuln assessment, and managed by the CC for the EDR solutions and any record or evidence that the ISMS Governs other regions. *The full reports could be found in **Annex C**.*

The requirement at Hays – Microsoft Defender EDR is only of the Sophisticated tool provided by Tech giant organisation Microsoft, and Hays ISMS and the SOC are Implementing this tool in order to secure our systems and get an advance alert if any potential attacks at Hays. By using this tool we are created our Cyber defense stronger than past, and this is absolutely necessary to carry out Hays's business without any interruption by intruders.

6.2.2. Browsing Plug-in Security Assessments (Plug-In SA) for the UK&I:

Function - Browsing Plug-in Security Assessments (**Plug-In SA**) is another sophisticated tool in the world, and this tool is used at Hays Plug-In security assessments. The request is raised by any **Stakeholders**, and they send it to the Security Operation Centre (**SOC**) for their review process then the SOC evaluate the particular query and provides a report to the ISMS team at Hays Global position for further review, which comes to Hays Cyber Security Manager (**CSM**) or Information Security Manager (ISO), and Hays ISMS team decide that whether they will approve the request or not, and of course, Hays ISMS team takes decision based on Hays Global Cyber & InfoSec Strategy and the ISMS Policy, and they approved after a careful consideration based on Hays **Risk Matrix**.

Implementation - Implementation - Browsing Plug-in Security Assessments (**Plug-In SA**) activities (**Practical Phase**) are provided in order to understand its readers how Stakeholders raise a request to the SOC and how the SOC

evaluates them and sends them to the ISMS team at Hays for the final decision. However, the documents below only give you an idea that how Browsing **Plug-In SA** performs but the whole Practical documents can be found in **Annex C** end of this Research Project.

Figure: 09 – Browsing Plug-in Security Assessment

HAYS Recruiting experts worldwide

EXECUTIVE-SUMMARY

Extension Name:	**GlossaryTech Chrome Extension**
Extension Description:	Glossary Tech is Google Chrome plugin which allows you to check technical terms used webpage in fast way
Execution Method:	Chrome automatically activates plugin and provide access to tabs and executes the plugin script on it.
External Connections:	29 URLS (Please refer to detail report)
Privacy Exposed in Data transmission	Few data transmission was found to be done over HTTP in clear text format.
External Emails founds	None
Permissions:	**Total – 2** • **cookies -** Access information about an HTTP cookie. • **tabs -** To interact with the browser's tab system and execute Script on tab when content match is found.
Background Script Execution:	**No**
Risk Classification	**Low**
Expected IMPACT	Plugin remains active on all webpage browsed in google chrome and store access HTTP cookie in user browser.
Report Summary	During the security assessment it was observed that the plugins has access to all [redacted] No special permission or elevated privileges was requested or obtained by plugin and its execution was found to be benign and in line with its intended purpose

Figure: 10 - Browsing Plug-in Security Assessment based on record/ docs/ evidence. *The full reports could be found in **Annex C**.*

The Requirement at Hays – Browsing Plug-in Security Assessments (**Plug-In SA**) tool and the best practice (Implementation) lies with Hays ISMS Policy, and it is absolutely necessary in order to evaluate and mitigate risks by the Hays ISMS team.

6.2.3. Pro-Active Monitoring of Hays's Asset by Splunk for the UK&I:

Function - Splunk is another sophisticated tool in the Tech world, and at Hays, we are using this tool in order to ***Analyse*** and ***Investigate*** data and information generated by Splunk on its Dashboard. The SOC team runs reports on Splunk, and it provides all sorts of Data and Information but if anything, suspicious or something goes wrong or any other anomaly then after a firm Investigation if the SOC found anything serious then they (SOC) remediate the issue. However, the SOC team always liaises with the ISMS team at Hays and provides these updates on their Daily Delta Call.

*(**Reference** – Splunk is our direct Service Provider and a specialist from Splunk conducts training for our Security Personnel in order to implement all facilities from its original site, the main site could be found below: https://www.splunk.com/)*

Implementation - By using Splunk the SOC proactively monitors Hays's assets for the UK&I. However, the documents below only give you an idea that how the Splunk tool performs but the whole Practical documents can be found in **Annex C** end of this Research Project.

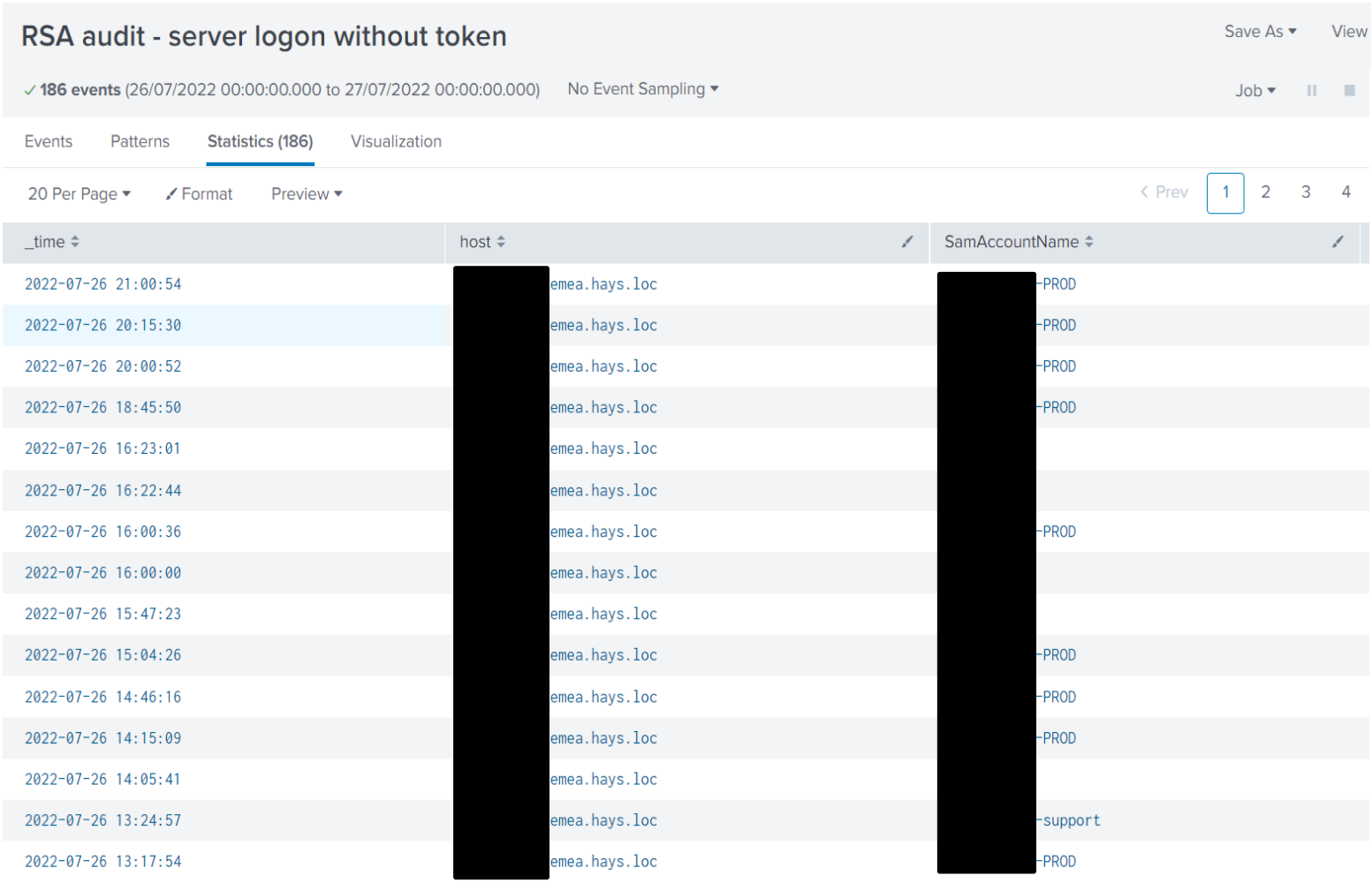


Figure: 11 - Pro-active monitoring of Hays's Assets by Splunk. The full reports could be found in **Annex C.**

The requirement at Hays - For Hays advance alert system pro-active monitoring is very necessary, and the Splunk tool provides Hays SOC and ISMS teams the level of confidence that if something goes wrong for their (Hays) asset then it will be showing on Splunk's radar, and the Dashboard will be providing much accurate information to keep secure Hays Cyber Defence and carry out Hays ISMS function.

6.2.4. Web Application Firewall monitoring (WAF) for the UK&I:

Function - Web – Application Firewall monitoring (**WAF**) is one of the sophisticated security tools in this Information Age. Because of this tool, the SOC is able to create a Demilitarised Zone (DMZ), which Isolated Firewall from Hays's main security gateway. However, by using this tool the SOC is able to set fine-tuning rules, fine-tune, and is able to look at that access who

is genuine and who is not, and the SOC decides and makes sure those genuine access is not blocked at Hays's resources. However, if something goes wrong then the SOC rectifies the issue and laisse with the ISMS team at Hays, but the SOC report to the ISMS team if anything changes, i.e. Management Change.

Implementation - Web – Application Firewall monitoring (**WAF**) activities (Practical Phase) are provided in order to understand its readers how the SOC is filtering, monitoring, and blocking any abnormal or malicious traffic at the Hays network. However, the documents below only give you an idea that how the **WAF** performs but the whole Practical documents can be found in **Annex C** end of this Research Project.

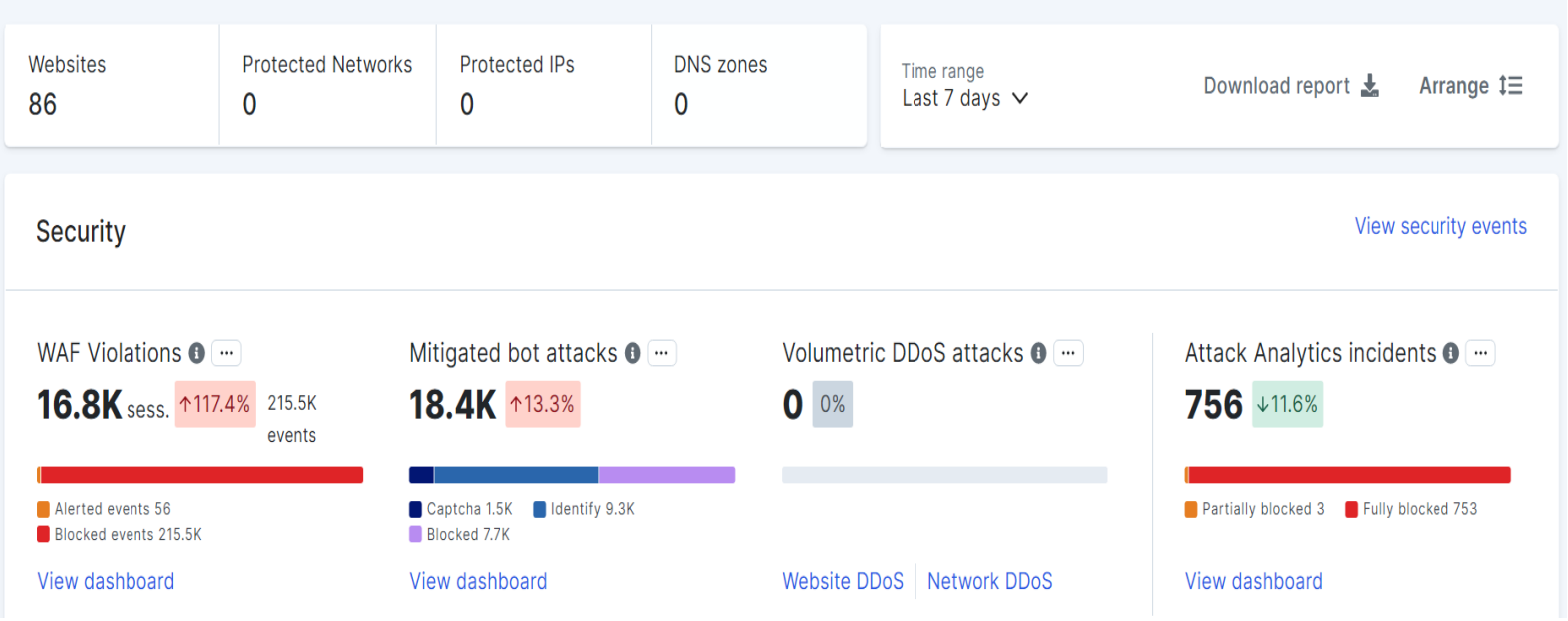


Figure: 12 - Web Application Firewall monitoring (as fine-tune, finetune rules, and others). *The full reports could be found in **Annex C.***

The requirement at Hays – This tool is very essential, as it operates and decides by the SOC who will be entering at Hays resources, which maintain the Confidentiality, Integrity, and Availability (CIA) triage within ISMS capability in order to keep fit Hays business forefront by providing their (Hays's users) **Availability** (**A**).

6.2.5. 3rd Party Risk Advisory for EMEA:

Function - From Hays Central and Global position Hays ISMS and the SOC liaise with other regions in order to implement any security tool to keep fit Hays business. EMEA liaise with the SOC and Hays's ISMS team before initiating any business with the **3rd Party Vendors** to review their IT Security Risk posture. IT SOC uses publicly available information in conjunction with the documentation by the vendors, and the responses to the security questionnaire to assess the IT risks posture and share advisory to the ISMS and Hays's business for them to make informed decisions.

It means, that if those regions want to do anything related to 3rd party business, then they use this 3rd party risk advisory tool and it goes to the SOC to review it, and then the SOC reviews the IT risk posture and then they (the SOC) give a **Green Signal** to the regional team to go ahead.

Implementation - **Could Monitoring** (3rd Party Risk Advisory) activities (**Practical Phase**) are providing in order to understand its readers how other regions (EMEA) if want to do anything with 3rd party business then how they reach out to the SOC and how the SOC review the IT risk posture for using 3rd Party tool at Hays for Cloud Monitoring solution, and how the SOC is maintaining all communications with Hays ISMS team, other regions and with the 3rd Party. However, the documents below only give you an idea that how **Cloud Monitoring** performs but the whole Practical documents can be found in **Annex C** end of this Research Project.

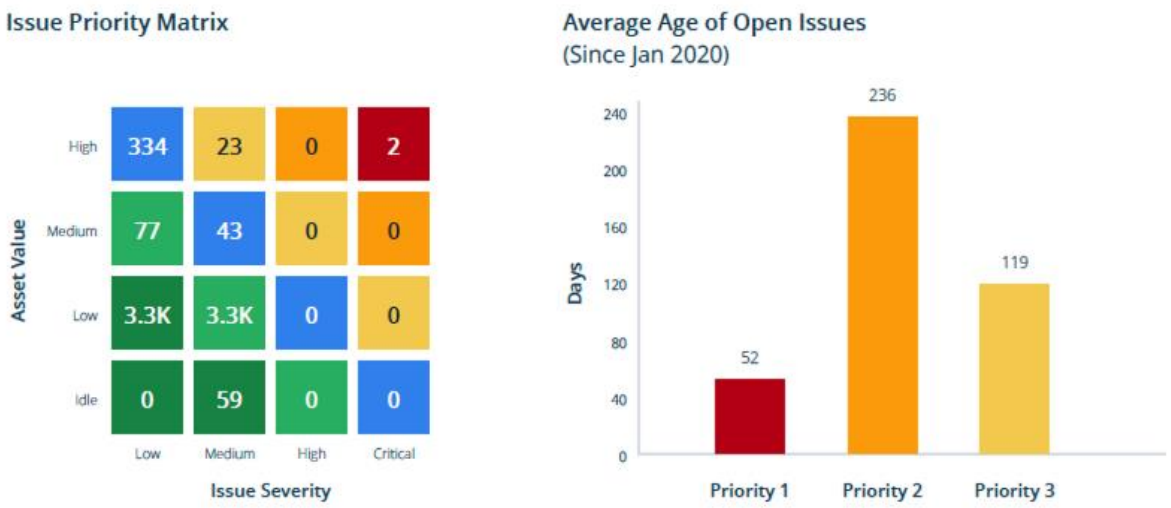
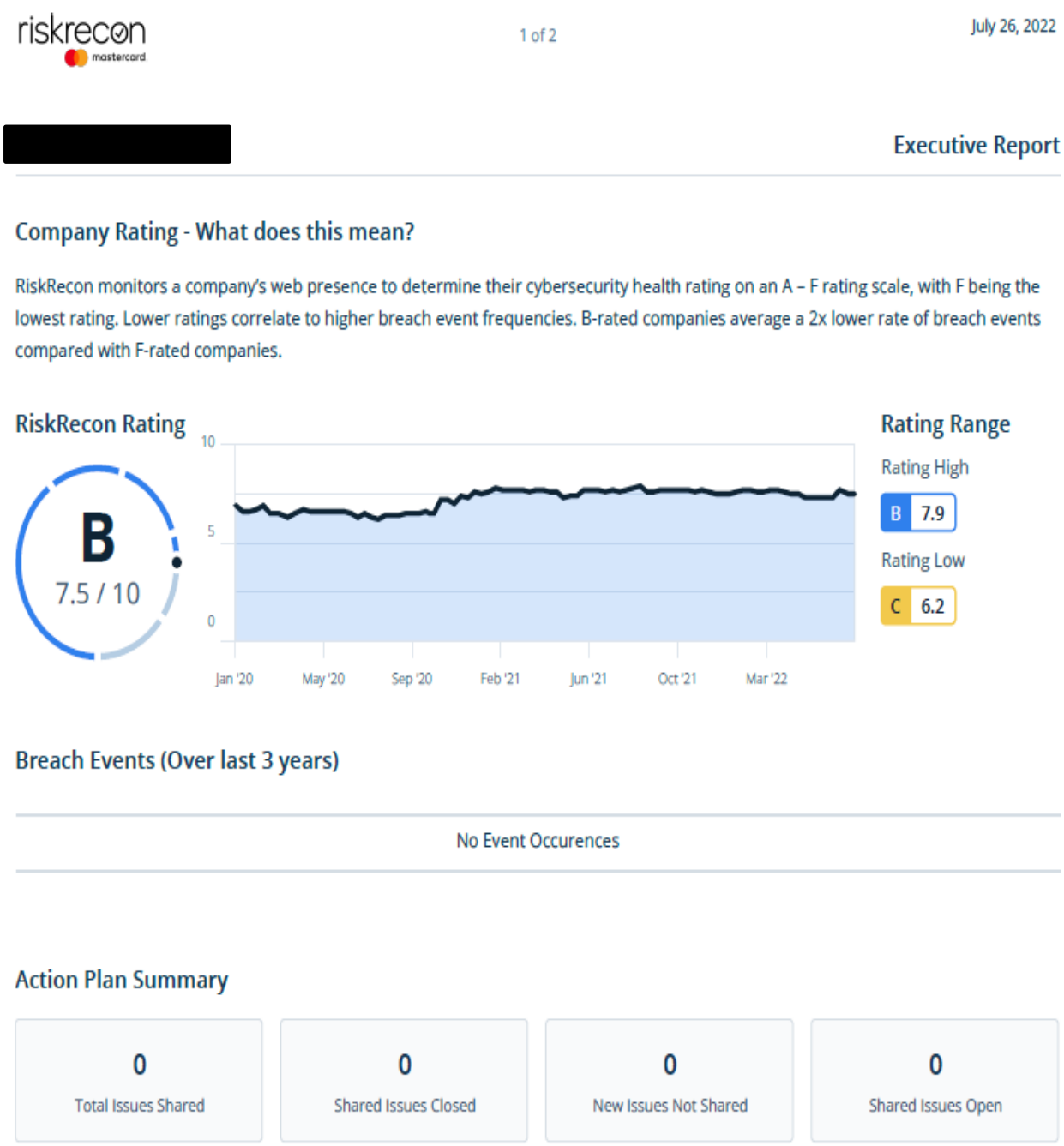


Figure: 13 – Priority Matrix by RiskRecon for Cloud Monitoring


riskrecon
mastercard

1 of 2

July 26, 2022

[redacted]

Executive Report

Company Rating - What does this mean?

RiskRecon monitors a company's web presence to determine their cybersecurity health rating on an A – F rating scale, with F being the lowest rating. Lower ratings correlate to higher breach event frequencies. B-rated companies average a 2x lower rate of breach events compared with F-rated companies.

RiskRecon Rating

B
7.5 / 10

10
5
0
Jan '20
May '20
Sep '20
Feb '21
Jun '21
Oct '21
Mar '22

Rating Range

Rating High
B 7.9

Rating Low
C 6.2

Breach Events (Over last 3 years)

No Event Occurences

Action Plan Summary

0	0	0	0
Total Issues Shared	Shared Issues Closed	New Issues Not Shared	Shared Issues Open

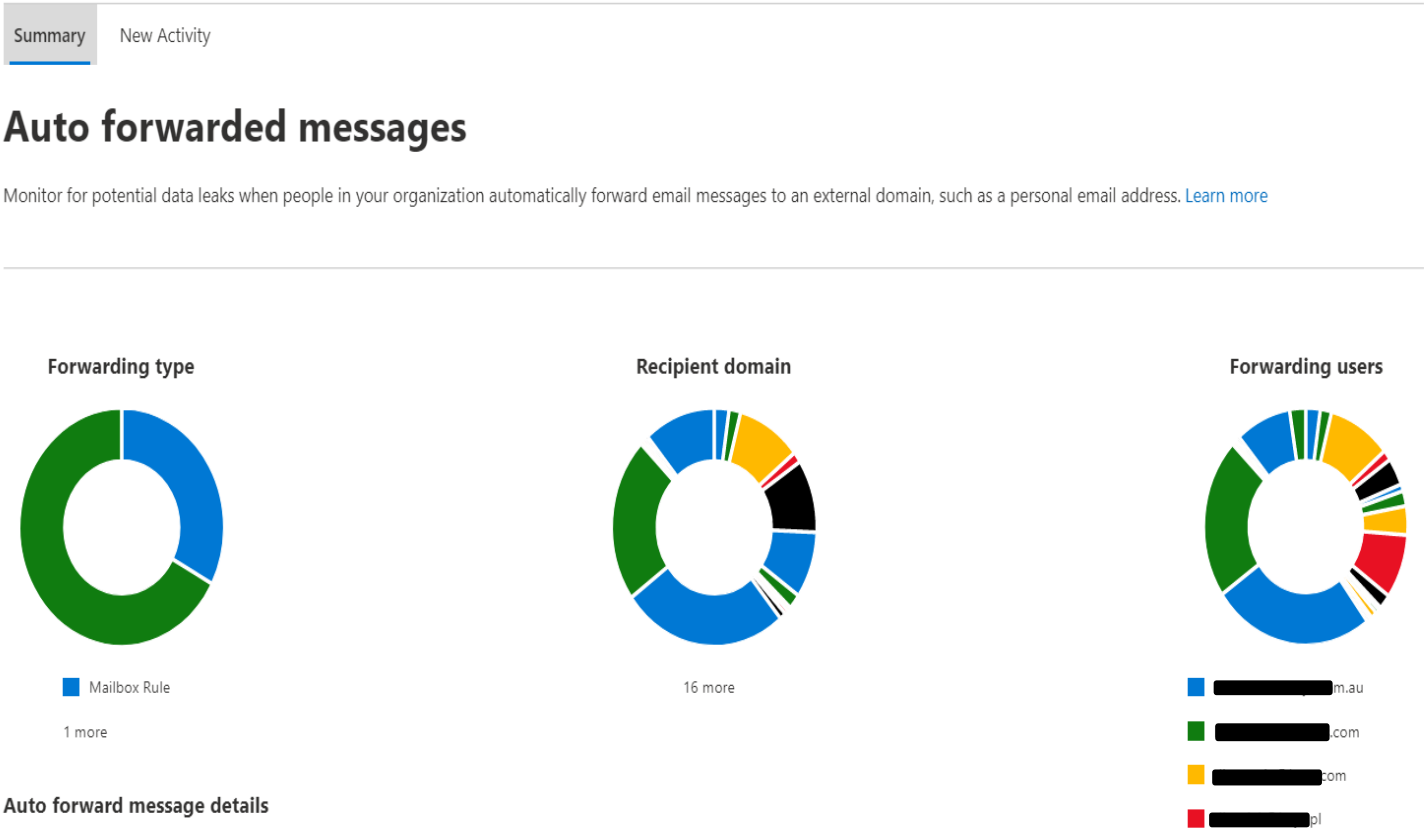
Figure: 14 – For EMEA by the 3rd party risk advisory. *The full reports could be found in* ***Annex C***.

<u>The requirement at Hays</u> – This tool is one of the finest tools for the 3rd Party Risk Advisory and very essential for Hays security monitoring of the 3rd party vendors Hays working with for its daily business; however, before implementing this tool each region must go through the SOC review process and the ISMS teams advise to make sure Hays Data and Information staying secure.

6.2.6. Office 365 (Security Monitoring) for the APAC:

Function – APAC uses the Office 365 tool, which is an Email Compliance System at Hays. Similarly, EMEA if APAC wants to do anything related to 3rd party business or in relation to **mail forwarding alert**, then they use this 3rd party risk advisory tool and go to the SOC for review it, and then the SOC reviews the IT risk posture and then they (the SOC) give a **Green Signal** to the regional team to go ahead, and again, the SOC establish a communication with the ISMS team at Hays for further advise in order to carry out its activities.

Implementation – **Office 365** (**Security Monitoring**) activities (**Practical Phase**) are provided in order to understand its readers how other regions (**APAC**) want to do anything with **Security Monitoring** how they reach out to the SOC and how the SOC reviews the IT risk posture for using 3rd Party tool at Hays for mail forwarding alert solution, and how the SOC is maintaining all communications with Hays ISMS team, other regions and with the 3rd Party. However, the documents below only give you an idea that how Office 365 performs but the whole Practical documents could be found in



Annex C end of this Research **Project.**

Figure: 15 – For APAC – Office 365 by the Security Monitoring. *The full reports could be found in **Annex C**.*

The requirement at Hays – This tool is one of the very important tools for 365 Office by the 3rd Party Risk Advisory and essential for Hays mail forwarding alert in order to maintain Hays business with outside of the

organisation; therefore, this tool is very helpful from the business prospect, as it is solving most of the critical issues in relation to mail forwarding at Hays business.

7. Global and Regional Projects of Hays ISMS:

Hays Group technology or Group Production Services IT recently approved a big budget (***total budget of Hays's IT is £45 million***) for the world's most leading and sophisticated tools to make Hays Cyber and IT Security job easier than before. Hence, Hays deployed a few tools and processes in order to carry out Hays Global Operations in Cyber and IT Security, and the ISMS and Cyber teams at Hays are responsible for those implementations. Those elucidating below:

7.1. Microsoft E5 Licence for Hays Global role:

Function and Implementation – Hays recently has Licenced Microsoft E5, and it replaces Microsoft E3 Licence at Hays by taking the license (MS. E5) Hays IT and Cyber Security moved many steps ahead for its (Hays) Cyber and IT security.

This **E5 Licence** costs around **"£7 million"** for a year, and every year Hays is paying this amount to Microsoft, and it is providing **protection across the attack kill chain**, and we as the ISMS team at Hays can Implement and achieve so many things by using this world's leading tool. This is not only restricted by one protection or Kill chain for Hays, but it can also, and it is performing for MS. Defender for Office 365 – protection across the kill chain, MS. Defender Endpoint – protection across the kill chain; similarly, MS. Defender for Identity – protection across the Kill chain, and MS Cloud App Security – protection across the kill chain.

The MS. E5 Licencing included Defender for Office, Azure Identity Protection, Defender for Endpoint, Defender for Identity, MS Defender for Cloud Apps, Protection Office 365, and many more (all features from Microsoft, as it is the highest privileged based on the Licencing).

This tool is performing from the Global position at Hays Central Services IT, also, performing from the regional IT offices, but it is correlating with all branches and regions to get the main output from the Global position, which helps the ISMS team at Hays to operate Globally in an orderly fashion.

The requirement at Hays – The MS. E5 Licencing is not only the solution for Hays Global Operations, Controls, and Security, but also it provides at Hays E5 Compliance, which is absolutely necessary for Hays Information protection and Governance, Insider Risk Management, eDiscovery, and Audit, and all these are directly linked with the ISO 27001 (Information Security Management System), ISO 27002 (Implementation of ISMS), and ISO 31000 (Risk Management) in order to achieve the ISO certification, as Hays is holding the ISO Certificate for the current year 2022.

This MS. E5 Licencing was the game changer for Hays ISMS and Cyber Security and re-shape Hays IT posture, which is helping Hays to carry out their business smoothly.

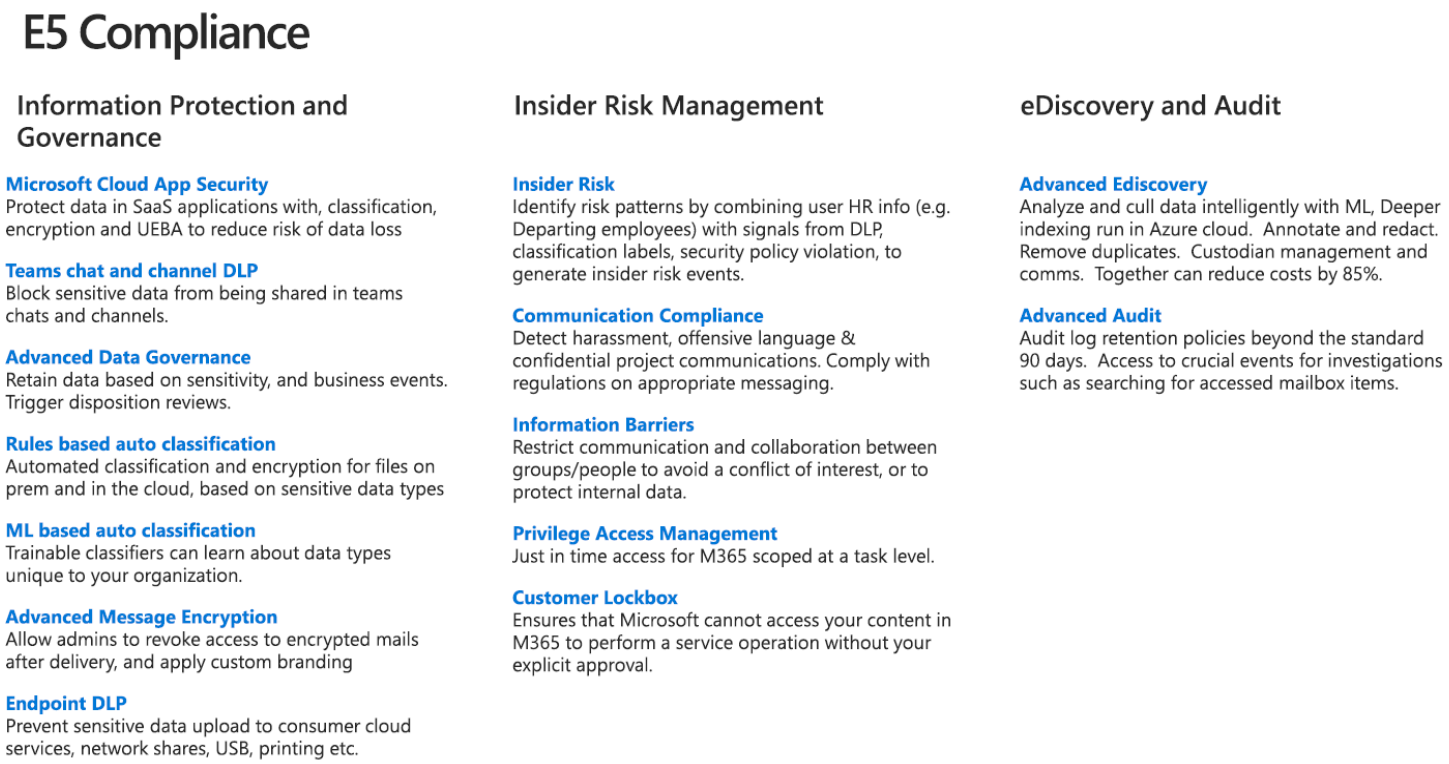


Figure: 16 – Microsoft E5 Licence is providing Compliance benefits at Hays.

7.1.1. Why it's (Microsoft E5 Licence) important to Hays:

The Microsoft E5 Licence provides a centralisation capability to Hays's Central Services IT, which means the ISMS team at Hays can **Monitor** and **Operate** from one place rather than operate from various places. Alongside this, by using **MS. E5 Licence**, Hays's ISMS and IT teams integrated into Microsoft's C-suite facilities which provide a peaceful security indication to the rest of the business at Hays (business with other parties and clients); especially, Hays's customers are able to see that how secure Hays's system is, how Hays protect their personal and sensitive data and maintaining a very good standard in this complex Cyber Age.

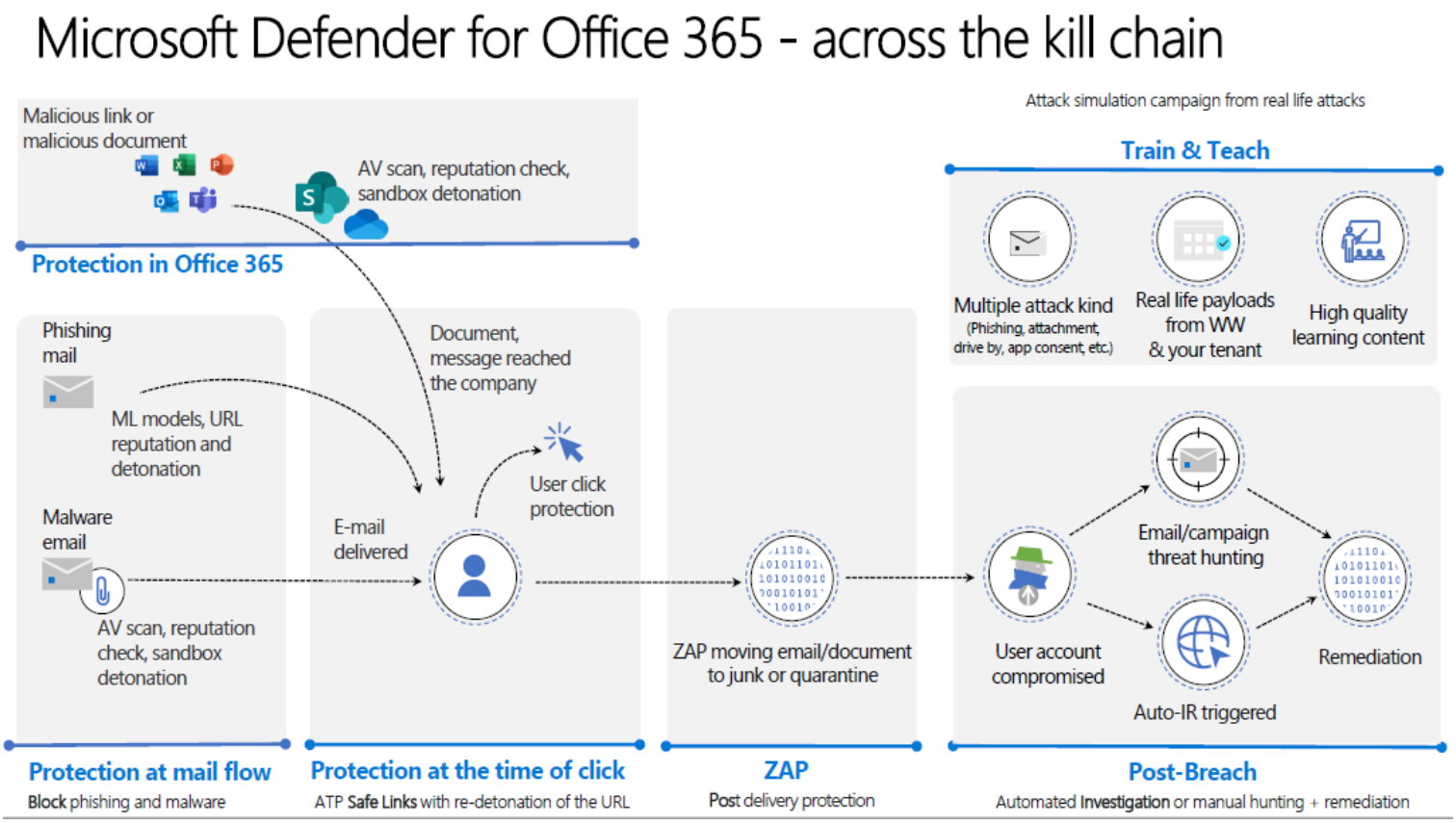


Figure: 17 – Microsoft E5 Licence is providing **protection across the attack kill chain**. *The full reports could be found in **Annex C**.*

7.2. Tenable SC (Nessus) Vulnerability Scanning Software for Hays Global role:

Function and Implementation – Hays recently deployed another world's sophisticated Vulnerability Scanning Software, which includes licensing for Nessus.

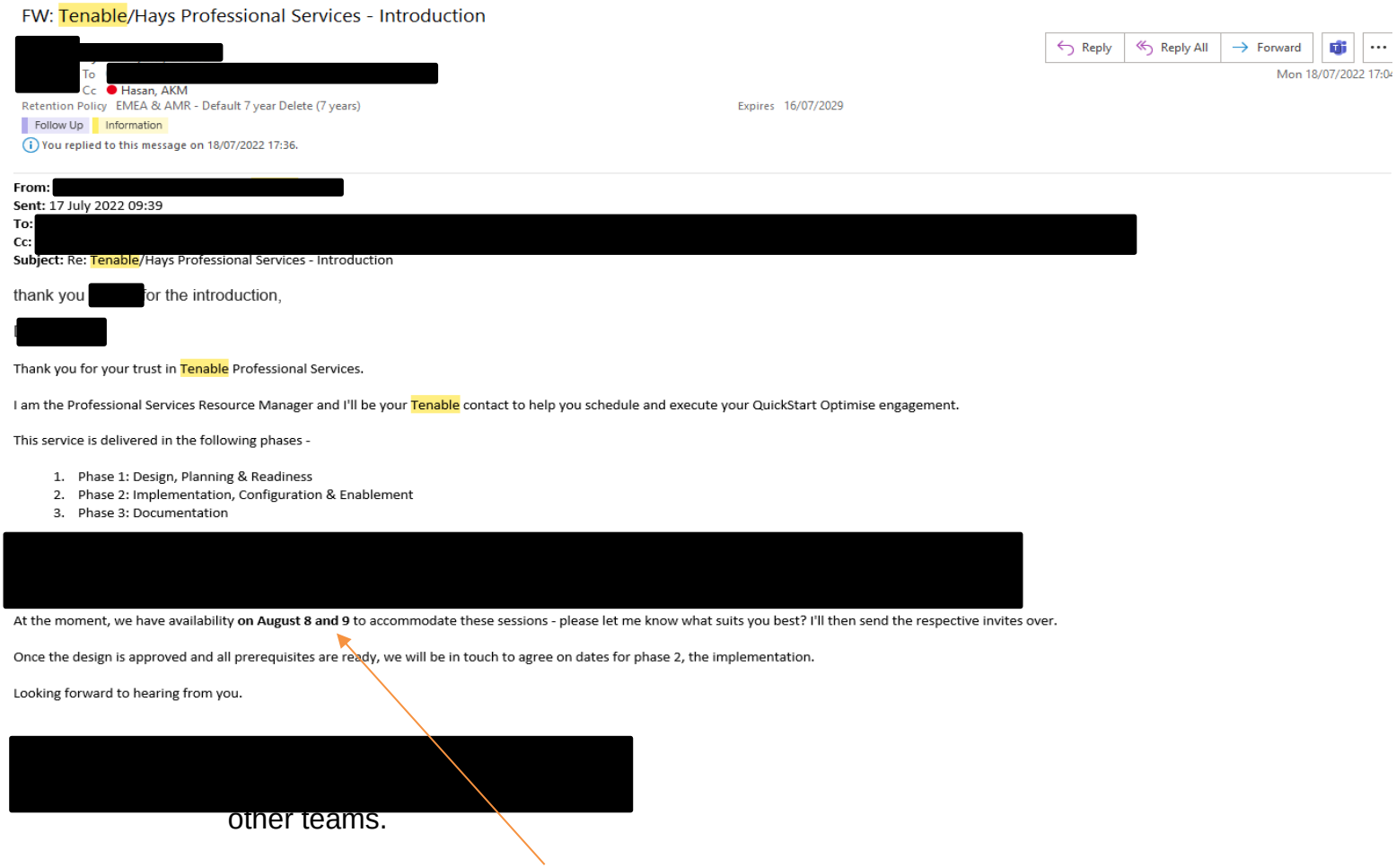
The main aim was from the ISMS team at Hays Global position that brings overall security under one umbrella, wherein this Tenable Software helped to do that, as every region has their own Dashboard for its Scanning, but Hays Central Services IT has a Master Dashboard where Hays ISMS team and Production Service Director would be able to observe and analyse if anything requires for Hays IT and Cyber security.

This software is able to scan for all-Global IPs; however, from the Service overview this software has 3 Phase, and those are below:

a) Tenable Design, Planning, and Reediness,
b) Tenable.io Implementation, Configuration, and Enablement,
c) Documentation and Project Coordination.

*(**Reference** – Figure 18 illustrates more about the Tenable Design and plan, and workshop training Phase; however, for the GDPR all sensitive email Dada and Information is hidden.)*

But all these things were achieved by the SOC and ISMS teams at Hays by conducting 2 and half-day workshops arranged by Tenable headquarters in London, which help both teams in order to cascade their training to regional and


FW: Tenable/Hays Professional Services - Introduction

[redacted]

To [redacted]

Cc Hasan, AKM

Retention Policy EMEA & AMR - Default 7 year Delete (7 years) Expires 16/07/2029

Follow Up Information

You replied to this message on 18/07/2022 17:36.

Reply Reply All Forward Mon 18/07/2022 17:0

From: [redacted]
Sent: 17 July 2022 09:39
To: [redacted]
Cc: [redacted]
Subject: Re: Tenable/Hays Professional Services - Introduction

thank you [redacted] for the introduction,

[redacted]

Thank you for your trust in Tenable Professional Services.

I am the Professional Services Resource Manager and I'll be your Tenable contact to help you schedule and execute your QuickStart Optimise engagement.

This service is delivered in the following phases -

1. Phase 1: Design, Planning & Readiness
2. Phase 2: Implementation, Configuration & Enablement
3. Phase 3: Documentation

[redacted]

At the moment, we have availability **on August 8 and 9** to accommodate these sessions - please let me know what suits you best? I'll then send the respective invites over.

Once the design is approved and all prerequisites are ready, we will be in touch to agree on dates for phase 2, the implementation.

Looking forward to hearing from you.

[redacted]

other teams.

Figure: 18 – Tenable SC workshop plan by Tenable for Hays's ISMS Managers and SOC team.

<u>The requirement at Hays</u> – By identify and doing Vulnerability Scanning from a Global position made Hays ISMS and the SOC life easier, but this tool is very sensitive, as the ISMS team at Hays is always careful about its Implementation, and of course, it's (Tenable) tuning and optimization provide Hays business more comfort than past and Hays ISMS team achieving more confidence day by day by Implementing this Tenable SC tool.

At the same time, it is a part of Scope that by using this tool, the ISMS team actually can document its output and Implementational steps, which must be helpful for an Internal and External Audit approach at Hays.

Figure: 19 – Tenable SC

2. SERVICE OVERVIEW

Tenable.io® Quick Start Optimize services is a tailored service beginning with a Design and Planning Workshop to plan, design and guide towards adopting the Cyber Exposure Lifecycle and Risk-Based Vulnerability Management (RBVM) practices through the configuration and integration of a fully operational capability of Tenable.io.

This Quick Start service develops an organizational RBVM approach, leveraging Tenable's enterprise platforms and services to reduce overall Cyber Exposure risk.

This Quick Start Optimize Implementation is designed across three (3) key phases within the scope defined in this Brief:

Phase 1: Tenable Design and Planning, and Readiness

- **Design and Planning.** Experienced Tenable Consultants ("Consultant") will perform a one-day design and architecture workshop with Customer to agree on a solution design according to Tenable Best Practice and recommendations.
- **Readiness Exercise.** Experienced Tenable Consultants ("Consultant") will review and validate the solution design, prerequisites and specifications before Phase 2 - Implementation and Enablement commences.

Phase 2: Tenable.io Implementation, Configuration and Enablement

- **Install sensors and configure Tenable.io.** Nessus® sensors will be installed and configured based on requirements and will implement following Tenable's best practices for enterprise deployment captured during Phase 1 - Design and Planning.
- **Validate operational capabilities.** Tenable.io will be validated end to end for scanning and other operational capabilities.
- **Enablement.** Experienced Tenable Consultants ("Consultant") will provide a Tenable.io Enablement session guiding you through Tenable's best practices for Vulnerability Management.

Phase 3: Documentation and Project Coordination

- **Tenable Deliverable Documents.** Include Design and Architecture Workshop deliverable and Tenable.io documentation of your specific configuration of Tenable products post Installation provided for your future use.
- **Project Coordination.** Experienced Tenable Consultants ("Consultant") will provide ongoing Project Coordination and

Figure: 20 - Figures 19 and 20 Tenable SC workshop by Tenable for Hays ISMS Managers and SOC team. *The full reports could be found in* ***Annex C.***

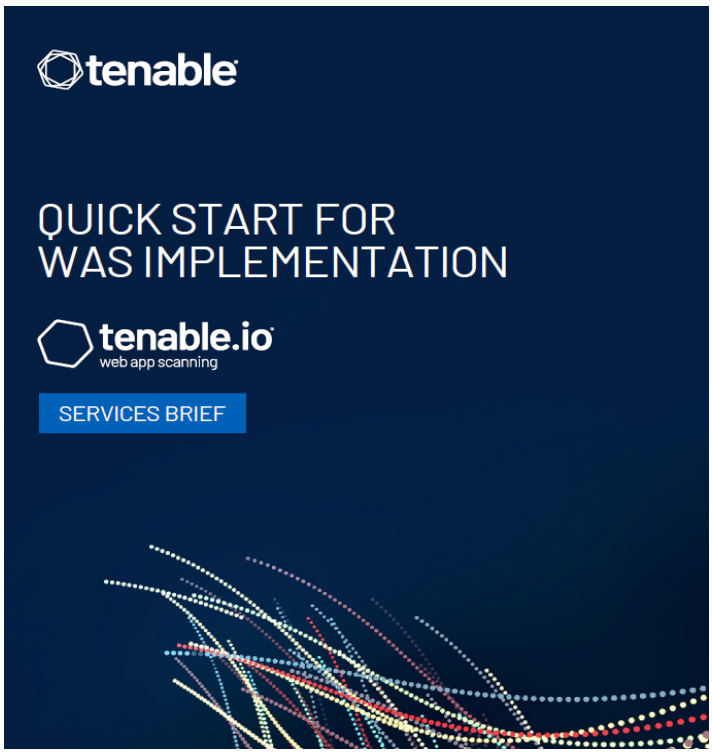
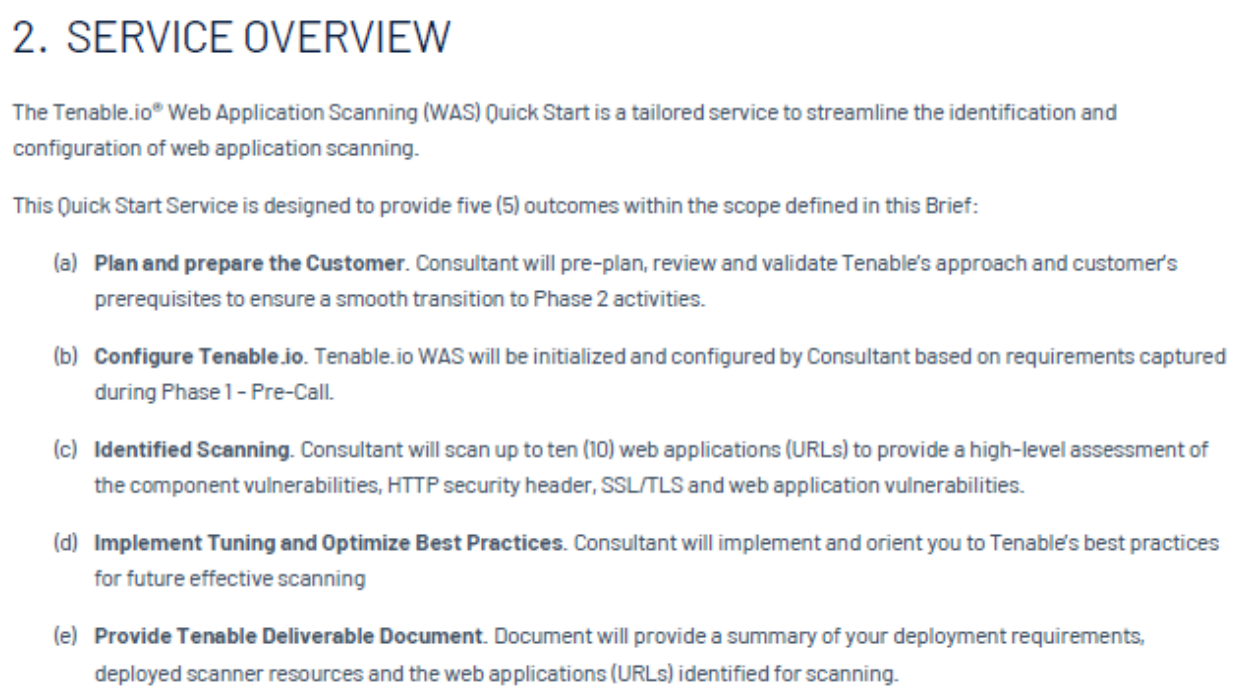


Figure: 21 – Tenable SC



2. SERVICE OVERVIEW

The Tenable.io® Web Application Scanning (WAS) Quick Start is a tailored service to streamline the identification and configuration of web application scanning.

This Quick Start Service is designed to provide five (5) outcomes within the scope defined in this Brief:

(a) **Plan and prepare the Customer**. Consultant will pre-plan, review and validate Tenable's approach and customer's prerequisites to ensure a smooth transition to Phase 2 activities.

(b) **Configure Tenable.io**. Tenable.io WAS will be initialized and configured by Consultant based on requirements captured during Phase 1 - Pre-Call.

(c) **Identified Scanning**. Consultant will scan up to ten (10) web applications (URLs) to provide a high-level assessment of the component vulnerabilities, HTTP security header, SSL/TLS and web application vulnerabilities.

(d) **Implement Tuning and Optimize Best Practices**. Consultant will implement and orient you to Tenable's best practices for future effective scanning

(e) **Provide Tenable Deliverable Document**. Document will provide a summary of your deployment requirements, deployed scanner resources and the web applications (URLs) identified for scanning.

Figure: 22 – Figures 21 and 22 Tenable SC workshop by Tenable for Hays ISMS Managers and SOC team. *The full reports could be found in **Annex C**.*

7.3. Implementing of Incident Response Management (IRM) by the ISMS team:

Function and Implementation – Previously, Hays had a Disaster Recovery (**DR**) Process and conducted only a few Incidents Response Management (**IRM**) Processes, but never had any Global Incident Response Management (IRM) Process before, but recently, in India, the Information Ministry changed their law, as of effect on *28 April 2022*; hence, it is absolutely necessary and required for Hays to Design, and Implement the Global IRM process, rather than regional practice, as Hays has business in India.

Therefore, the ISMS team at Hays Central Services IT created a new Playbook for the Global IRM process in conjunction with the Head of IT at Hays in India. This IRM playbook and the bundle (all documents) will describe everything to each security team at Hays that how to perform and tackle any potential data breach or security incident at Hays; however, all Policies for the IRM in place at Hays and this IRM Playbook merely guide those Policies.

The requirement at Hays – The intention of this IRM Process is to justify and escalate the strength of Hays ISMS and IRM teams. By doing this simulation exercise in 2022, it will show a pen-picture to the Hays ISMS team where or which area or team needs to develop in order to tackle any security Incidents or data breaches at Hays.

At the same time, this IRM exercise challenges each team to prove how secure their areas are and how efficient they are during crisis moments at Hays; moreover, this IRM process provides Hays the ***change management*** based on the new law sets by the Government of India in April 2022.

*(**Reference** – Figure 23 illustrates more clarity about the Incident Response Management (**IRM**) Process Overview and design; however, the full documents could be found in Annex C.*

HAYS Working for your tomorrow

[redacted]

IRM PLAN and overview

Hays IRM plan/ Incident Response Management Plan (Updated version for 2022 [redacted] Guidelines and Directions for the Overall IRM Desktop Exercise.

When an incident or potential incident take place at Hays, whether it is related to data breaches or security-related issue, then it triggers the IRM process, and then the relevant teams and Personnel start their process, as per the IRM Playbook.

All procedures and steps are in place at Hays for the IRM, but these IRM documents are extra precautions for Hays Cyber and ISMS team to oversee the process, as a whole in a simpler and faster way.

[redacted] on the real-world scenario, and in order to (IRM related) must be prepared and well [redacted]t or manage the incidents.

For the next Phase follow document 01 - a) >>

Figure: 23 – Incident Response Management (**IRM**) Process Overview provided by the ISMS team at Hays. *The full IRM process could be found in **Annex C.***

SCENARIO:
A Hays user has reported to the Service Desk that he has tried to open a document on a shared drive. The document has not opened correctly and the screen is displaying a message.

What happens now?

We follow through on the Hays "Breach scenario flowchart".

Figure: 24 - Figures 23 and 24 Incident Response Management (**IRM**) Process at Hays and the ISMS team is responsible for that. This scenario was extracted from Hays's last Top table Exercise for the IRM process. *The full reports could be found in **Annex C**.*

8. Project Management and Risk:

This Research Project is focusing on conducting and completing research-based activities on Hays tools and technologies within its Central Services IT department. Hence, the risk factors are extreme, which falls into a Major category and the likely chance is 50% - 90% (50% of scheduled based on the risk matrix) because to complete the project will be utilising Hays Data, Information, and a lot of outputs, including reports and Incident Reports via some sophisticated tools at Hays.

*(**Reference**: Figure 25 illustrates more clarity about the Risk Assessment for this project at Hays, which was extracted from Google to compare how many risks are in it in it and why its category is **extreme** in order to finish this Project at Hays.)*

Therefore, to manage this project, it is better to be very careful about those elements and factors when utilising to complete this Research Project, and alongside this, during any movement around the Coventry University campus, any public place, and even within the Hays building I must take care of those, i.e. Laptop, Hard Drive, USB sticks, reports from tools, email conversation and design for all Phase.

However, if I lose any Data or Information about Hays, it is required to inform the ISMS team at Hays, and the ISMS team will be registering these incidents in Hays's Data Loss Prevention (DLP) file, if things go very severe then they (Hays) might follow the investigation path in order to mitigate the risks for Hays's business. Hays have designated Personnel in order to conduct this DLP process, but this process lies with Hays ISMS and Data Security Policy.

Likelyhood	Consequences				
	Insignificant *Risk is easily mitigated by normal day to day process*	**Minor** *Delays up to 10% of Schedule Additional cost up to 10% of Budget*	**Moderate** *Delays up to 30% of Schedule Additional cost up to 30% of Budget*	**Major** *Delays up to 50% of Schedule Additional cost up to 50% of Budget*	**Catastrophic** *Project abandoned*
Certain *>90% chance*	High	High	Extreme	Extreme	Extreme
Likely *50% - 90% chance*	Moderate	High	High	Extreme	Extreme
Moderate *10% - 50% chance*	Low	Moderate	High	Extreme	Extreme
Unlikely *3% - 10% chance*	Low	Low	Moderate	High	Extreme
Rare *<3% chance*	Low	Low	Moderate	High	High

Figure: 25 – *Risk Assessment for this project at Hays, which was extracted from Google to compare how many risks are in it and why its category is* ***extreme*** *in order to finish this Project at Hays.*

9. Project Outcome:

By Auditing approach and revising all existing Auditing (by PWC, KPMG) could mitigate more risks than we can assume; therefore, "Digital Security Risk and Audit Management" is the best solution and good outcome for Hays Global position and other regions.

Additionally, the exiting Adulting report from PWC has suggested Hays change management is required, and by doing the Global IRM process it is giving an indication to external Auditing teams that Hays already started and currently conducting Operations and Implementation based on the Change Management and based on "Hays Global Cyber & InfoSec Strategy".

Moreover, this report will be a Business Report for Hays Central Services IT, and this report for security prospects of Hays ISMS team, which includes Cybersecurity and Information security at the Hays in order to test Hays Cyber and Information Security strength.

10. Recommendations:

Hays Central Services IT, and as a whole has most of the facilities for its Cyber and IT defense; however, by doing this Research project at Hays's Global position, and based on its "Global Cyber & InfoSec Strategy (Vision part)" I would recommend a few things toward Hays Cyber and Information security. Those are given below:

- Hays Strategic team (**ISMS**) or the SOC team are not using the **MITRE ATT&CK** navigation tool yet, but I am recommending using this tool, as it makes life easier for security teams if they want to identify attackers' behaviours and patterns by customising this brilliant tool. Additionally, this tool is able to provide recommendations (what to do) to defensive teams at the same time when it picks up the attacker's pattern.

- Security Orchestration, Automation, and Response (**SOAR**) solution could be another fantastic tool for Hays security teams, as it mainly focuses on 3 key areas, Vulnerability Management (**VM**), Incident Response (**IR**), and Security Automation, which means these coming under one umbrella for all operational and Implementation prospect.

- Whatever the ISMS process is done by the Cyber and Information Security Managers at Hays, it must be following Development and Continues process in order to maintain its (ISMS) Security Life Cycle.

However, by conducting this Research Project, the main threats and risks have been identified and evaluated correctly, including a recent real-Phishing attack in APAC on 01 Jul 2022 (Please see the Secondary Methodology, Annex A-C, and Phishing attack scenario in Annex C), and all security teams have rectified all findings (from all reports by all software and assessments), it means all evaluation has been completed Successfully in ISMS capability.

Moreover, the ISMS team has conducted some evaluations based on Hays Risk Matrix and ISO, see below:

- The Risk Assessment has been completed in conjunction with ISO 31000.
- The Implementation has been completed based on ISO 27001 and ISO 27002.
- The operations and controls have been completed based on NIST 800-53.

Alongside this, before at Hays wasn't any Global Cyber and Information Security Strategy, and I have recommended them; therefore, "Hays Global Cyber & InfoSec Strategy" has been established (Please see Primary Methodology).

And also, after I reviewed the Audit report by PWC (please see Annex B), I recommended them for Change Management, which was the new Incident Response Management (IRM) process, and now that has been established at hays, and it is operating globally for the IRM process.

Whatever, I have extracted in this Research Project, Implemented at Hays, and also, established at hays, I have maintained the GDPR, followed all current laws for InfoSec, and achieved those goals, as per my aim and objectives in this Research project.

11. Conclusion:

Everything I have done at Hays, and for this Research Project thus far is directly linked with my recommendation part of this Project; however, if the ISMS team at Hays focuses on their ISMS Policy and Implements that are based on “Hays Global Cyber and InfoSec Strategy” then the ISMS team would be able to conduct their Planning, Designing, Implementation, Enforcement, and Operational parts in order to mitigate the most significant risks to create Hays Cyber and Information defense posture. By doing all these the ISMS team at Hays can achieve their short, medium, and long-term goals in this competitive Information Age.

12. Appendices:

All Appendices used for this research project are given below:

Hays Global Cyber & InfoSec Strategy
Hays ISMS Policy
Hays SOC Policy
Hays CC Policy
Hays Network Policy
Hays Information Security Lifecycle
Hays Strategic Context
Hays Implementation Context (ISO 27002)
Hays Operational Context (NIST 800 family)
Hays Controls Context (NIST 800 – 53)
Hays Communication Context
Hays Enforcement Context
Hays 3rd Party Liaison Context
Hays Tools (all, but the name is proved in the Reference part of this Research Project)
Hays Auditing Context
Hays Vulnerability Assessment Context (Internal and External)
Hays Cyber and Information Defense Context
Hays Information Security Context (ISO 27001)
Hays GAP Analysis
Hays Risk Matrix (ISO 31000)
Hays IRM Context
Hays Licencing Context (with 3rd Party, i.e. Microsoft and Tenable)

Alongside this, **Appendices** – ***All other factors*** (in ***Annex A, B, and C***) have been captured in **Appendices** in this Research Project.

13. Annex A:

For this Research project whatever I have mentioned thus far in the Primary Methodology and Secondary Methodology (the practical part), including Global and Regional projects, everything provides in **Annex C** sequentially, including documents in **Annex B**.

However, I am explaining in **Annex B** a few ISMS activities, which did not mention in either **Primary** or **Secondary Methodology** these are not exact activities at Hays in-house scope, as these are previously conducted and currently conducted by 3rd Party organisations for Hays.

Annex A merely indicates and provides clarity about **Annex B** and **Annex C**, wherein **Annex C** is holding all the documents for this Research project at Hays Central Services IT.

14. Annex B:

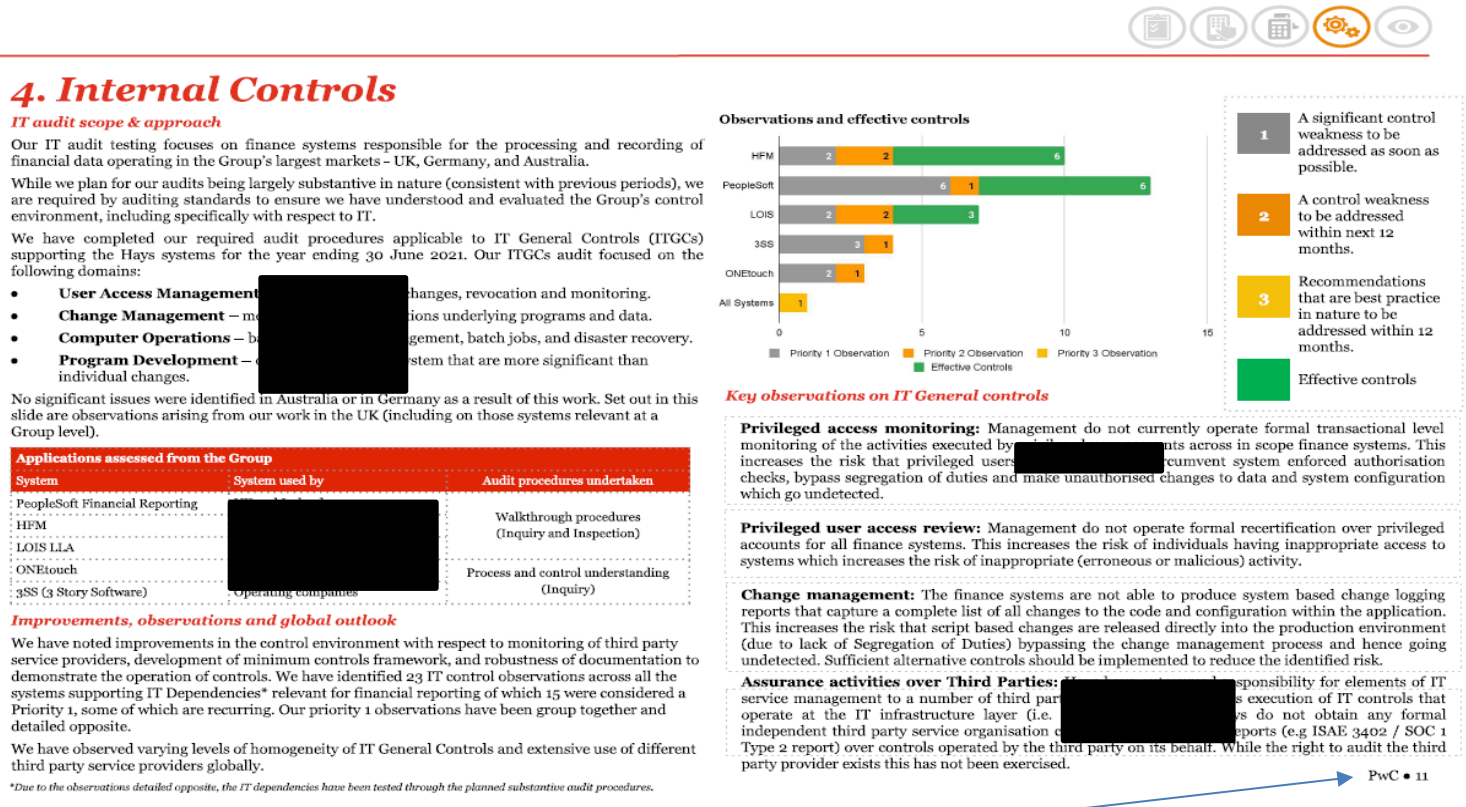
14.1. External Audit Trail at Hays:

Hays not only have Internal Auditing Approach based on its ISMS Policy and ISO 27001, but it also has an external Auditing Approach. Therefore, the ISMS team at Hays contacted the external bodies and arranged to conduct Audits in order to keep fit Hays's business and security posture forefront.

Hays contacted PWC in 2020 and 2021 to conduct an external Audit at Hays, this external party has conducted an Auditing from the Global prospect at Hays and provided their view, and they recommended a few changes for the security scope at Hays. Subsequently, the ISMS team at Hays Implemented their recommendation and changes their (Hays security posture) process, i.e. PWC recommended the Change Management, and the Hays ISMS team implemented the Global IRM process at Hays.

Similarly, KPMG has conducted an external Audit at Hays for Exiting Penetration Testing Advisory review, and they provided their recommendations, and the ISMS team acted on it to secure their IT structure.

The external Auditing sample is given below, but the full reports can be found in **Annex - C** like other documents.



4. Internal Controls

IT audit scope & approach

Our IT audit testing focuses on finance systems responsible for the processing and recording of financial data operating in the Group's largest markets – UK, Germany, and Australia.

While we plan for our audits being largely substantive in nature (consistent with previous periods), we are required by auditing standards to ensure we have understood and evaluated the Group's control environment, including specifically with respect to IT.

We have completed our required audit procedures applicable to IT General Controls (ITGCs) supporting the Hays systems for the year ending 30 June 2021. Our ITGCs audit focused on the following domains:

- **User Access Management** – [redacted] hanges, revocation and monitoring.
- **Change Management** – m[redacted]ions underlying programs and data.
- **Computer Operations** – b[redacted]gement, batch jobs, and disaster recovery.
- **Program Development** – [redacted]stem that are more significant than individual changes.

No significant issues were identified in Australia or in Germany as a result of this work. Set out in this slide are observations arising from our work in the UK (including on those systems relevant at a Group level).

Applications assessed from the Group		
System	System used by	Audit procedures undertaken
PeopleSoft Financial Reporting	[redacted]	Walkthrough procedures (Inquiry and Inspection)
HFM		
LOIS LLA		
ONEtouch		Process and control understanding (Inquiry)
3SS (3 Story Software)	Operating companies	

Improvements, observations and global outlook

We have noted improvements in the control environment with respect to monitoring of third party service providers, development of minimum controls framework, and robustness of documentation to demonstrate the operation of controls. We have identified 23 IT control observations across all the systems supporting IT Dependencies* relevant for financial reporting of which 15 were considered a Priority 1, some of which are recurring. Our priority 1 observations have been group together and detailed opposite.

We have observed varying levels of homogeneity of IT General Controls and extensive use of different third party service providers globally.

**Due to the observations detailed opposite, the IT dependencies have been tested through the planned substantive audit procedures.*

Observations and effective controls

1 A significant control weakness to be addressed as soon as possible.

2 A control weakness to be addressed within next 12 months.

3 Recommendations that are best practice in nature to be addressed within 12 months.

Effective controls

Key observations on IT General controls

Privileged access monitoring: Management do not currently operate formal transactional level monitoring of the activities executed by [redacted]nts across in scope finance systems. This increases the risk that privileged users [redacted]cumvent system enforced authorisation checks, bypass segregation of duties and make unauthorised changes to data and system configuration which go undetected.

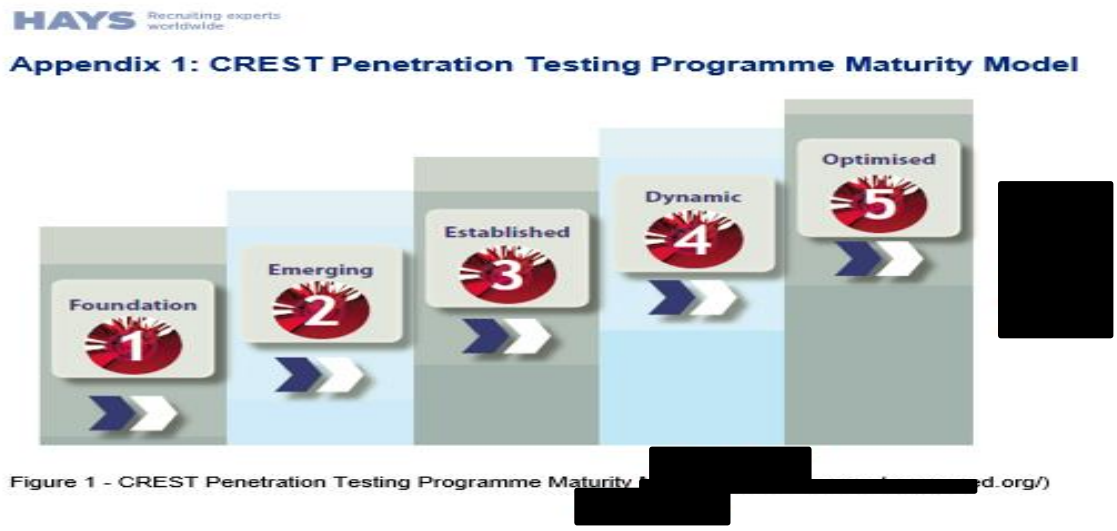
Privileged user access review: Management do not operate formal recertification over privileged accounts for all finance systems. This increases the risk of individuals having inappropriate access to systems which increases the risk of inappropriate (erroneous or malicious) activity.

Change management: The finance systems are not able to produce system based change logging reports that capture a complete list of all changes to the code and configuration within the application. This increases the risk that script based changes are released directly into the production environment (due to lack of Segregation of Duties) bypassing the change management process and hence going undetected. Sufficient alternative controls should be implemented to reduce the identified risk.

Assurance activities over Third Parties: [redacted]sponsibility for elements of IT service management to a number of third par[redacted]s execution of IT controls that operate at the IT infrastructure layer (i.e. [redacted]s do not obtain any formal independent third party service organisation c[redacted]eports (e.g ISAE 3402 / SOC 1 Type 2 report) over controls operated by the third party on its behalf. While the right to audit the third party provider exists this has not been exercised.

PwC • 11

Figure: 26 – An External Auditing by **PWC** arranged by the ISMS team is responsible for that. *The full reports could be found in **Annex C**.*



HAYS Recruiting experts worldwide

Appendix 1: CREST Penetration Testing Programme Maturity Model

[redacted]

Figure 1 - CREST Penetration Testing Programme Maturity [redacted]d.org/)

Figure: 27 - An External Auditing by **KPMG** for an Advisory Review arranged by the ISMS team is responsible for that. *The full reports could be found in **Annex C**.*

14.2. Vulnerability Assessment Reports (Internal and External) at Hays:

The ISMS team at Hays not only seating down for an in-house scanning process by the SOC team, but they arranged to conduct Internal Vulnerability Assessments by A&O IT Group, which is a 3rd Party organisation to conduct Internal Vulnerability scanning process.

They conduct their scanning within the Scope at Hays, which is normally provided by the ISMS and SOC teams to the 3rd party organisation. After their Internal Vulnerability scanning, they provide reports to the ISMS team at Hays, based on those reports the ISMS team liaises with the SOC team, and the SOC team enforces on behalf of the ISMS team to relevant teams to rectify those security gaps or Vulnerabilities, i.e. close ports, Patch Management.

Similarly, the ISMS team at Hays arranged external Vulnerability Assessments by the NCC Group in order to make a strong Hays Cyber and Information defense posture. After their (NCCG) findings, the SOC Governance on behalf of the ISMS team to the relevant team to rectify those issues.

Reference *– Figures 28 and 29 provided the* ***Internal Vulnerability scanning*** *sample, which is extracted from* ***Q&A IT Group's*** *Scanning Reports, but the full reports could be found in* ***Annex - C*** *like other documents.*

	A	B	C	D	E	F	G	H	I	J	K	L
1	Scan Date	Scanner	IP Address	Tag	OS	Discovered Name	System Owner	Description (Asset register)	Hays Rating	Vulnerability Category	Vulnerability Title	Protocol / Port
2	May-22	qualys	[redacted]	Manchester	EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux	hrmnxpd4075	CC	RFW [redacted]	Low	Patch Maintenance and	.user.ini File Information Disclosure Vulnerability	[redacted]
3	May-22	qualys		Manchester	Windows 2012 R2/8.1	hrmvmpd3406.e	CC	Com	Low	Patch Maintenance and	Account Brute Force Possible Through IIS NTLM Authentication Scheme	
4	May-22	qualys		Manchester	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-	INFO Not Found	CC		Low	Data Transport	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	
5	May-22	qualys		Romford	Microsoft Windows 10	hrrvmpd4832.er	CC	R04	Low	Patch Maintenance and	Account Brute Force Possible Through IIS NTLM Authentication Scheme	
6	May-22	qualys		Manchester	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-	INFO Not Found	CC		Low	Services	Deprecated SSH Cryptographic Settings	
7	May-22	nessus		Manchester	AIX 7.1	hrmmgam06	CC	AIX	Low	General	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	
8	May-22	nessus		Manchester	AIX	hrmmgam06-pr	CC	AIX	Low	General	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	
9	May-22	nessus		Manchester	VMware vCenter Server Appliance 6.7.0 build	hrmmgvc030	CC	RFW App	Low	General	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	
10	May-22	qualys		Manchester	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-	INFO Not Found	CC	INFO Not Found	Low	General	Intelligent Platform Management Interface (IPMI) Detected	
11	May-22	qualys		Manchester	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-	INFO Not Found	CC	INFO Not Found	Low	Patch Maintenance and	OpenSSH "child_set_env()" Security Bypass Issue	
12	May-22	qualys		Manchester	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-	INFO Not Found	CC	INFO Not Found	Low	Patch Maintenance and	OpenSSH "X SECURITY" Bypass Vulnerability	[redacted]

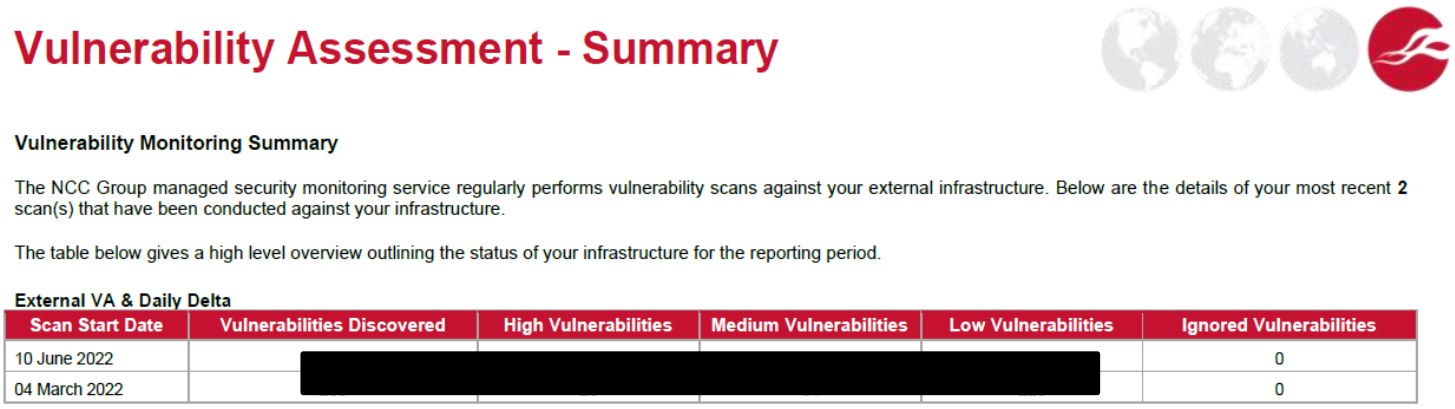
Figure: 28 – Internal **VA** by Q&O IT Group

O	P	Q	R	S
CVSSv2	**CVE**	**Diagnosis**	**Recommended Solution**	**Data Collected**
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	N/A	Since PHP 5.3.0, PHP includes support for ="https://secure.php.net/manual/en/configuration.file.per-user.php" TARGET="_blank">.user.ini configuration files	Customers as advised to protect their .user.ini files from unauthenticated access by implementing security solutions	Sensitive .user.ini file detected on port: 443. GET /.user.ini HTTP/1.0 Host: 10.50.83.26
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	CVE-2002-0419	NTLM authentication is enabled on the Micros	Currently there are no vendor supplied patches available for this issue. Workaround 1) Disable NTLM	GET / HTTP/1.0 Host: [redacted] Authorization: NTLM TlRMTVNTUAABAAAAA7IAAAAAAAAAAAAAAAD
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	CVE-2016-2183	Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support	Disable and stop using DES, 3DES, IDEA or RC2 ciphers. More information can be found at: "https://www.t22.info/"	CIPHERKEY-EXCHANGEAUTHENTICATIONMACENCRYPTION(KEY-STRENGTH)GRADE SSLv2 WITH 64 BIT CBC CIPHERS IS
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	CVE-2002-0419	NTLM authentication is enabled on the Micros	Currently there are no vendor supplied patches available for this issue. Workaround 1) Disable NTLM	GET / HTTP/1.0 Host: [redacted] Authorization: NTLM TlRMTVNTUAABAAAAA7IAAAAAAAAAAAAAAAD
6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)	N/A	The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another. The target is using deprecated SSH	Avoid using deprecated cryptographic settings. Use best practices when configuring SSH	Typename key exchangediffie-hellman-group1-sha1 cipher3des-cbc cipherblowfish-cbc
7.5	CVE-2022-22719		Upgrade to Apache version 2.4.53 or later.	
7.5	CVE-2022-22719		Upgrade to Apache version 2.4.53 or later.	

Figure: 29 - Figures 28 and 29 Internal Vulnerability Reports by A&O IT Group. *The full reports could be found in **Annex C**.*

Reference *– Figures 30 and 31 provided the **External Vulnerability scanning** sample, which is extracted from **NCC Group's** Scanning Reports, but the full reports could be found in **Annex - C** like other documents.*

Figure: 30 – External VA by NCC Group



Vulnerability Assessment - Summary

Vulnerability Monitoring Summary

The NCC Group managed security monitoring service regularly performs vulnerability scans against your external infrastructure. Below are the details of your most recent **2** scan(s) that have been conducted against your infrastructure.

The table below gives a high level overview outlining the status of your infrastructure for the reporting period.

External VA & Daily Delta

Scan Start Date	Vulnerabilities Discovered	High Vulnerabilities	Medium Vulnerabilities	Low Vulnerabilities	Ignored Vulnerabilities
10 June 2022	[redacted]				0
04 March 2022					0

Figure: 31 – Figures 30 and 31 External Vulnerability Reports by NCC Group. *The full reports could be found in **Annex C**.*

14.3. Penetration Testing at Hays:

Penetration Testing or Pen Testing is an advanced testing approach for any organisation in order to check their Security Strength, Vulnerability, and Security Gap. Likewise, the ISMS team at Hays organised Penetration Testing to evaluate their security gap.

Hence, the NCC Group recently conducted Penetration Testing within the scope at the Reading office, UK. After their test and finding the NCC Group sent this to the ISMS team at Hays and advised to mitigate some risks and some risks could be accepted by the ISMS team.

Reference *– Figures 32, 33, and 34 provided the* ***Penetration Testing*** *sample, which is extracted from* ***NCC Group's*** *Pen Testing Reports, but the full reports could be found in* ***Annex - C*** *like other documents. However, this* ***(Pen Testing)*** *is* ***181 pages*** *document, but it is provided in* ***Annex C*** *very begging and end in order to concise this Research Project.*

Therefore, the IT Production Services Director is involved with the ISMS team and Hays's Cyber Security Manager that whether it is possible to remediate those risks based on the NCCG, and if needed how can the (IT Director) could accept any risk; the Cyber Security Manager (who is the author of this project) and the ISMS team remediate all risk and provided advice to the Director to accept One risk based on the ISMS teams GAP assessment and Hays Risk Matric (Exact Data and accepted risk is not available due to Hays Security and Commercial Policy).

The penetration Testing and Remediation sample are given below, but the full reports can be found in **Annex - C** like other documents.

Figure: 32 – Penetration Testing Reports by NCC Group. *The full reports could be found in* ***Annex C****.*

1 Executive Summary

This report presents the findings of the zero trust network security assessment conducted on behalf of Hays Specialist Recruitment (Hays). The assessment was conducted between 14/03/2022 and 18/03/2022.

The system being assessed was part of Hay's move away from the traditional trusted office design to a zero-trust Internet connected design. This model has been initially piloted in two offices although the security assessment was carried out in a single location, the Reading office.

Overview

The security posture of the systems within scope was found to be appropriate to the assets which required protection. However, it was also noticeable that the majority of the risk to the network was presented by a small number of the observed devices. A number of high risk issues were identified which should be addressed if the organisation's security model is to maintain an appropriate defence in depth basis. The findings also illustrate the importance of ensuring that an otherwise robust security model cannot be undermined by isolated weaknesses.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
External Infrastructure	[redacted]				
Internal Infrastructure					
Total					

Assessment Summary

The security assessment was split
perspective and testing from an int
a minimal set of services were exp
for attack and no security weaknes
further split into an initial phase of
which made use of information pro
number of networks, some of whic
poor IT practices and the observed
which should not be exposed.
[redacted]

Figure: 33 – Penetration Testing Reports by NCC Group. *The full reports could be found in **Annex C**.*

ICO Programme - Pen Test Management Response

A Pen test was carried out by NCC Group at Reading office post the proof-of-concept conversions of both [redacted]. The results of these findings have been delivered by NCC Group to Hays and stored in full in SharePoint here.

Below is a table of the High and Medium issues found during the exercise, some commentary, suggestions for closing the issue, the Owner of the issue and the management response:

Finding	Commentary	Management Response	Owner
1. HIGH – Paxton MSSQL	This is [redacted] per point 4.	Acknowledged, ICO Programme will mitigate only. [redacted]	ITPS to [redacted] resolution
2. High – default net2 credentials	This is unrelated [redacted] properties must [redacted] remediate this re[redacted] location. ITPS wil[redacted] per point 4.	Acknowledged, ICO Programme will mitigate only. [redacted] s and	ITPS to [redacted] resolution
3. High – Passwords on physical media	Shared password[redacted] limitation of our [redacted]	Acknowledged, but IT cannot prevent a repeat. [redacted] once	ITPS Device [redacted]
4. High – Door entry exposed	Difficult this one. [redacted] to be connected t[redacted] allow remote acce[redacted] and to permit use[redacted] identification from[redacted]	Acknowledged, ICO Programme will mitigate only. [redacted] result from work for ICO.	ITPS Device [redacted]

Figure: 34 – Figures 32, 33, and 34 Penetration Testing Reports by **NCC Group**. *The full reports could be found in **Annex C**.*

15. Annex C:

Annex C captured all documents, software, and tools utilised for this Research Project. Everything is explained above in this Project, but in Annex C their further details are provided sequentially. See below:

Figure 01 - Hays IT and Cyber functioning Clockwise, this document is extracted from Hays's Cyber Security Manager's Operational diary and roadmap. This figure is given in **Paragraph Number (3) Background,** and see below**:**

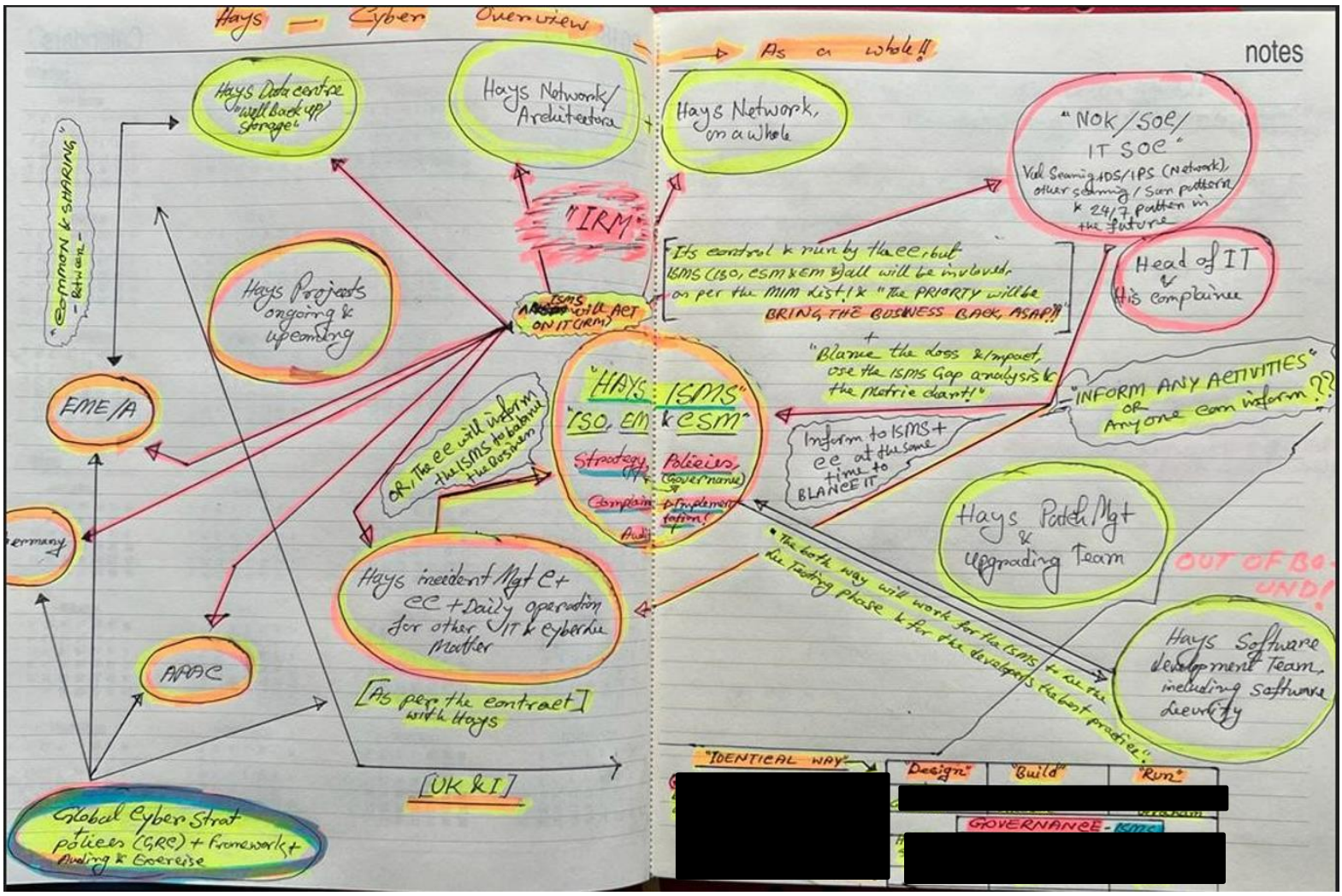


Figure: 02 – "***Hays Global Cyber & InfoSec Strategy***", this whole document is extracted from Hays Global Cyber & InfoSec Strategy itself. Data has been hidden for GDPR purposes. This figure is given in **Paragraph Number (5) Primary Methodology for Hays ISMS Project.**

However, this is 15 pages document but given a few of them to understand how is "*Hays Global Cyber and InfoSec Strategy*" and how the ISMS team Implements and Enforces based on this. Black masks cover data and Information due to GDPR and Hays's Commercial Confidentiality Policy. These documents are given below:

HAYS Working for your tomorrow

HAYS GLOBAL CYBER & INFOSEC STRATEGY

SECURING HAYS INFORMATION

HAYS Working for your tomorrow

CONTENTS

Pillar 5: [redacted]

Pillar 6: [redacted]

Delivering Hays Ambition and Completing the mission

Cyber Resilience

Understand Cyber Risk

Risk Analysis

Scope for Implementation

Control, Monitoring

Frameworks

Cyber Security Implementation Procedure

Incident Response Management (IRM) Process

Annex A: Cyber and InfoSec as parts of Hays Global Agenda

Annex B: ISMS Regulations - Hays Strategy

[redacted]

Annex C: Glossary

Document History

Version	Date	Author	Modifications
0.1	[redacted]22	[redacted] (Hays ITSecO)	[redacted]
0.2	[redacted]Jun 22	AKM Hasan (Hays CSM)	2nd draft version by changing structure and points.
0.3	[redacted]n 22	AKM Hasan (Hays CSM)	3rd draft version by changing structure, narratives, context, and points.
0.4	14 Jul 22	AKM Hasan (Hays CSM)	4th version draft
0.5	[redacted] 22	AKM Hasan (Hays CSM)	Final version draft
0.6	[redacted]Sep 22	AKM Hasan (Hays CSM)	Minor changes and re-shape the final version
0.7	[redacted]Sep 22	AKM Hasan (Hays CSM)	The final version of Hays Global Cyber Security Strategy
0.8			

Document Review & Approvals

Version	Date	Reviewed by	Approved by	Comments
0.7	[redacted]Sep 22	[redacted]		Approval from IT Ops Director
0.8	[redacted]Sep 22	[redacted]		Approval from GCTO

HAYS Working for your tomorrow

Introduction

Challenges of the digital age and Hays opportunities

Technology is evolving, and this is the most important moment for Hays to move forward with Cyber and Information Security strategic goals in this digital age. This Strategy sets out at a high level, the agreed approach to respond to and mitigate as far as possible the Cyber and Information risks with the appropriate framework, controls, authorities, actions, and implementation plans. The Strategy is designed to support the efforts to Detect, React to and Defend against Cyber and Information threats and risks and highlights the organisation, its processes, and technological responses needed to support the strategy at a global level, as well as regional level.

Purpose of Hays Cyber and InfoSec Strategy

This Strategy will establish a solid roadmap for Hays Global Cyber and Information Security at all levels in relation to IT, Cyber, Data, and Information, which will help Hays (all regions, branches, and any liaison between Hays and other parties) to come on common ground and drive forward Hays Cyber and Information Security to keep Hays IT Infrastructure fit and continue Hays business forefront without any interruption.

Alongside this, the strategy works with the IT Enterprise Risk Management process that identifies, evaluates, and manages Cyber Information risks at a global level for Hays. To mitigate **High** to **Low** risks, this Strategy must be followed by ISO 31000. It is also informed and kept relevant with input from various other sources including audit reports (internal and external), threat intelligence, security incidents, alerting, and trends from monitoring systems and external sources; this strategy must be followed by ISO 27001 and ISO 27002 in order to maintain ISMS of Hays and it's implementation.

Moreover, this strategy must be followed by NIST 800 - 53 controls families, set prescriptive guidelines, and provides firm directions and methodology for establishing standard operating procedures (**SOP**), details can be found later in this Strategy in the Frameworks section.

Goals of the Global Cyber and InfoSec Strategy and Scope

This document is designed to set out the high-level Global Cyber and InfoSec Strategy for Hays with a vision until 2030; however, its reviewing process will be dictating and will be changed its **short**, **medium**, and **long-term** goals, and also, it will depend on business necessity, legislation, and latest technology.

It sets out the Goals Cyber and InfoSec overview in order to carry out the Cyber and Information function at Hays, as well as the underlying main pillars that underpin the strategic approach to cyber and Information security, as a whole.

[redacted]

HAYS Working for your tomorrow

In addition, this Global Strategy initiated to support those **2 parts** are listed in this document. These will be updated and approved periodically by the responsible Personnel in conjunction with all Global Cyber and InfoSec leaders at Hays. This high-level Global Strategy sets some goals with its Cyber and InfoSec vision in **Part 1**, and the other part more focuses on its **Implementation**, which is agreed upon by all Global Cyber and InfoSec leaders and Global Cyber and InfoSec Committee at Hays; it elucidates everything in the Scope part of this Strategy.

Part 1: Strategy

Hays Strategic Context

Hays Cyber and InfoSec Landscape

This strategy is like an umbrella for overall Cyber and Information Security at Hays; also, this document provides Directions to all policies related to IT, Cyber, and InfoSec in order to conduct any IT Audit. Risk Assessment, ISMS evaluation, and Decision-Making Process, IT, Cyber, and ISMS team, as well as other purposes for this Strategy, the relevant parts of the document, could be shared with external parties for the purposes of bids and tenders or risk assurance activities. Hence, this document provides some firm Directions and Guidelines (G&D) in Governance (Control and Monitoring) for Hays Cyber and InfoSec, Framework, Scope (depending on the circumstances), Authorities, Implementation, and its reviewing process.

This Strategy is based on **2 Parts**; **Part 1** sets out the "**Strategy**", and **Part 2** sets out Hays "**Implementation**", and subsequently, organised under **6 Pillars**, which is the focal point for this document in order to keep the momentum for the Cyber and Information security at Hays. However, those **6 Pillars** define the Cyber and Information security function at Hays.

Hays Cyber and Information Security

[redacted]

All policies under this Strategy in relation to Cyber and Information security concepts are well described, but this document merely provides a synopsis of it. Those are below:

- [redacted] Security Management System (ISMS)
- [redacted] Security Standard
- [redacted] Security [redacted]

Alongside this, they will be providing their views, and recommendations based on current threats, vulnerabilities, security development, framework, implementation, and enforcement of Hays in conjunction with all other policies, projects, and operations.

Enforcement

[redacted]

Therefore, the Global Cyber and Information security Strategy enables all Cyber and Information Security managers to enforce both **Parts** of this Strategy in order to carry our Hays IT and Cyber security function, as a whole based on ISO (ISO 27001, ISO 27002, ISO 31000) and NIST standard (NIST 800 – 53, NIST 800 – 53 A and NIST 800 – 53 B).

Furthermore, this Strategy provides directions to all policies related to Cyber and InfoSec, and any violation of this Global Strategy will lead to consequences based on policies.

Part 2: Implementation

Hays Global Cyber and Information Security and its 6 Pillars

The Global Cyber and Information Security Strategy at Hays has been developed as a result of the current Cyber threats presented and in response to the Cyber Risks that Hays has identified that are directly relevant to its operations.

This Strategy sets **6 Pillars** to reinvigorate Hays's Cyber and Information security Implementation and Operations, and at the same, this document enables its Cyber and Information security Managers and Leaders to enforce their responsibility to achieve the goals and also, be adept at managing and remediating security incidents while working and promoting a culture of security awareness with an adversarial approach to improve Cyber defensive postures of Hays. Those **6 Pillars** are:

Pillar 1: [redacted]

[redacted]

[redacted]

That is why the [redacted] the business needs and are relevant [redacted] model and culture – "IT Security ar [redacted] t the same time, utilising our Subj [redacted] e to support business lines a [redacted] and Information security recomm [redacted] ays function based on ISO 27001 and 27002 Framework.

Pillar 2: [redacted]

[redacted] ecisions will [redacted] identification,

Therefore, [redacted] lines and Directions (G&D) for t [redacted] roper Risk Assessmer [redacted] ISO 31000 Framework [redacted], in order to conduct the [redacted] goals and all relevant de [redacted] operate with Hays Cyber and InfoSec Personnel.

Pillar 3: [redacted]

Communication [redacted] yber InfoSec team and for the [redacted] participating in regular meetin [redacted] foSec Committee, Secu [redacted] nce forums, and regular catch [redacted] g Meetings, Project Meetings [redacted] ack, opinion, representing coo [redacted] Cyber Information Security team to assess and mitigate Cyber and Information Risks at Hays.

Alongside this, each team related to IT, Cyber, and InfoSec must be open up, cooperate and execute a delegated task for Hays Cyber and Information security; any IT, Cyber, and Information security-related task must be conducted by a work agreement (verbally or written) within timelines, and this document enables all leaders at Hays Cyber and Information Security to carry out their responsibility to accomplish their tasks for each event.

Pillar 4: [redacted]

This document provides better clarifications about all policies under this Strategy, and this Global Strategy provides directions to all policies in regard to the Point of Contact (**POC**), Course of Action (**CoA**), and Chain of Control (**CoC**).

[redacted]

HAYS Working for your tomorrow

[redacted]

[redacted]

Hays allocated skill set Personnel with responsibilities, and those are responsible to liaise with those organisations and maintain this process in order to tackle the emergency situation.

[redacted]

[redacted]ponsible for the physical security, and all policies are in place to maintain this.

[redacted]

[redacted]Hays IT and InfoSec by physical security, and they have the on-guarding system in place, and Hays's designated Personnel (i.e. ISO) ensure that the physical security and all other security in place based on ISO 27001.

Alongside this, those teams are maintaining the GDPR and all other equivalent laws (i.e. The Privacy Act 1988) based on local laws and legislation.

[redacted]

Implementation of a global set of CA rules that will control access from mobile and laptop devices dependent on where and how they are connecting. Active blocking and enforcement of access policies will be implemented on a globally consistent basis.

Global real-time vulnerability scanning

Review of options to implement a single, global, real-time vulnerability scanning capability. To be implemented globally but operated locally so each regional IT team can ensure the integrity of their local environment based on a global set of policies. Comparison between Qualys and Tenable solutions is being undertaken with a recommendation to the security teams and then to the GCTO for approval, which is in progress and it will be potentially operational in September 2022.

[redacted]

Review of options and costs to implement a service in Outlook for end-u[redacted]cam emails and receive feedback on w[redacted] with 3 options are being considered ([redacted] and evaluation is underway for costs and service. This is still in progress in order to reinvigorate Hays's Cyber defense posture.

[redacted]

13

HAYS Working for your tomorrow

E5 Licencing

Microsoft E5 Licensing is giving Hays an extra boost in order to monitor and create an extra layer of security. By using sophisticated tools and techniques everything will come under one umbrella from the Cyber and InfoSec point of view. Hays deploying this tool in Jul, but it will b operational from September 2022.

Frameworks

Implementation of a common set of minimum-security controls that are consistent across all regions, and in line with the ISO 27001 framework. The initial Phase of this ISO series (ISO 27000) is assessing the current control framework and performing a **gap assessment chart** against ISO 27001 that what and how the risk matrix presents the potential risk at Hays, and Phase 2 will agree with the common controls required as the minimum standard, and its (ISO 27001) control procedure (Annex A), and it is vital to implement the control procedure ISO 27002, which provides the guidelines for the implementation of control listed in ISO 27001, and it could be leading to local implementation in each region of any that are missing.

Alongside this, Hays must arrange an internal auditing process by implementing 114 Annex A of ISO 27001. This Global Cyber and InfoSec Strategy provides guidelines for a suitable IT, Cyber, and InfoSec auditing approach, and implement all other frameworks, as per risk assessment they (frameworks) should and must enable themselves to implement the Global Strategy for prioritising Information about security risks in order to mitigate high risks and potential attacks, to mitigate High to Low risks, this Strategy must be followed by ISO 31000 to maintain ISMS of Hays and it's implementation.

Moreover, this strategy must be followed by NIST 800 - 53 controls families, set prescriptive guidelines, and provides firm directions and methodology for establishing standard operating procedures (SOP) to apply security controls across Hays Global and Regional IT in the Cyber and Information security matters.

Cyber Security Implementation Procedure

Each and everyone working at or with Hays and their job roles related or not related to the IT, Cyber, and Information Security of Hays, still must comply with the Implementation Phase based on this Global Strategy in order to maintain the standard of Cyber and Information Security.

Incident Response Management (IRM) Process

Information Technology supplier and/or vendor shall be involved in the incident response process, including the relevant IT security incident processes.

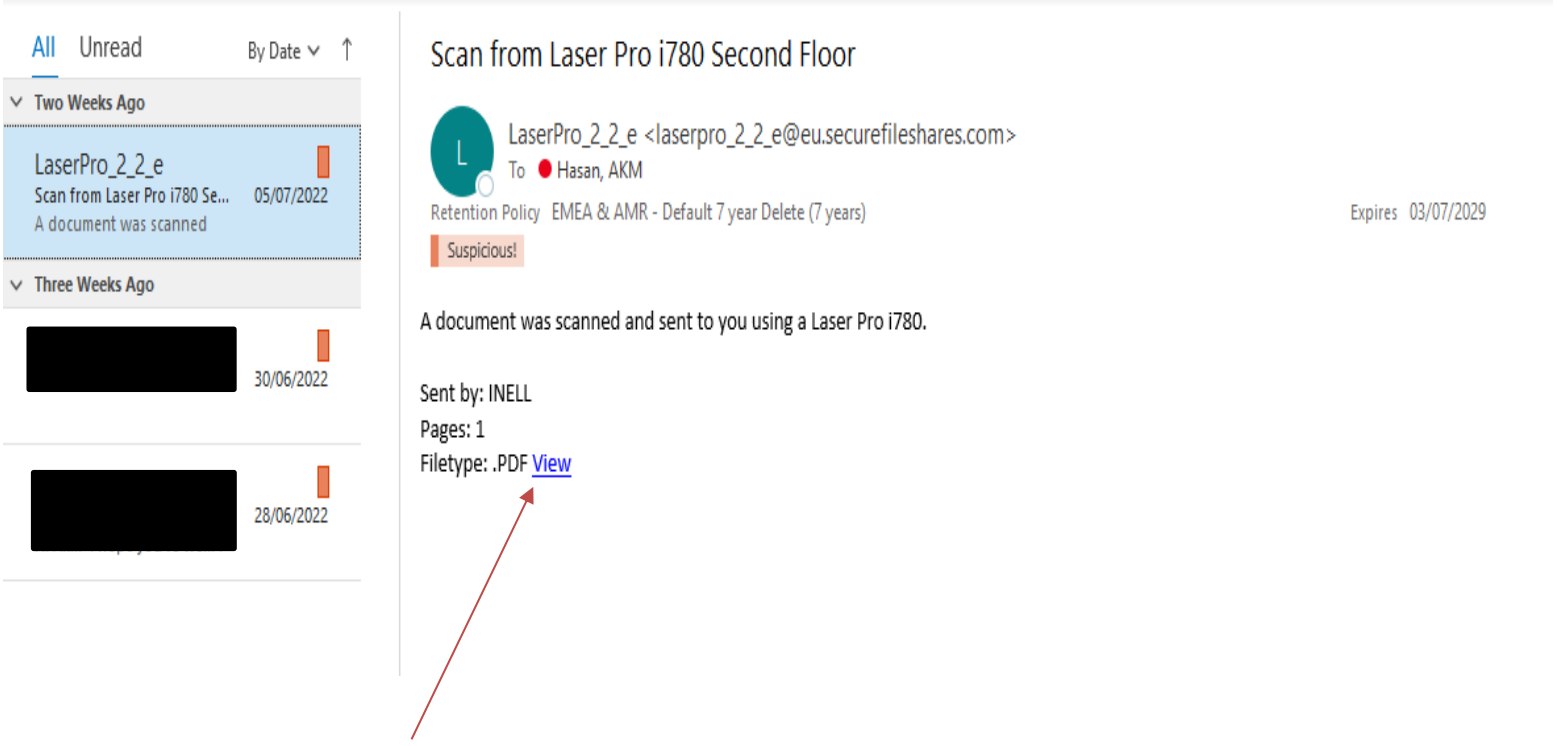
Whenever an incident compromises Hays' cyber security or has the potential to compromise Hays' Cyber or Information security, it must be immediately [redacted]

14

<u>Under Figure 02</u> - Phishing Simulation Test Running by Hays's ISMS Team, which is explained in **Aim and Objectives in Paragraph number (4)** and also, under the ***Strategic Context*** and ***Implementation*** of Hays's Operations.

This document adding based on the Primary Methodology above in this project. This document is showing a "live Phishing" email, which is a Phishing link, which automatically goes to Hays suspicious folder in Office 365, I can not click it, as this is a live link, but if anyone clicks this link by mistake then they (whoever clicks) have to go through a mandatory Phishing awareness training at Hays.

Moreover, this is a **real-Phishing "*Simulation*"** Email; hence, I did not click the email but the whole email, and activities (Phishing Simulation) are given below:



***"The Simulation Phishing Link"** is Hays's Phishing Simulation Test by the ISMS team for all employees.*

However, on **01 Jul 2022**, an employee clicked **a REAL PHISHING EMAIL** in the APAC region, users clicked on ***a phishing link*** and provided all credentials.

Being the Cyber Security Manager of Hays Global Position (who is the Author of this Research Project), it is vital responsibility to deal with this realistic scenario.

We immediately contained the incident by blocking the sender's email address on ***Mimecast*** and resetting both the user account's password and the Office 365 token.

Moreover, the attachment that was embedded in this suspicious email was considered to be malicious by the **sandbox**.

All activities are provided below without any figure number, but the Sandbox Cloud reports are ***65 pages*** long, hence, providing a few of them to understand how Hays's security team (ISMS) cope in this **REAL Security Incident**.

Due to Commercial purposes, GDPR and APAC law, all sensitive data and Information are not available but for understanding its (this project) reader, I am adding a few steps Hays's security team conducted as soon as the employee clicked the link by attackers.

All activities (***LIVE PHISHING***) **sequentially** are given below:

Hi

It contains signatures associated with e.g. HtmlPhish10 according to the Yara open-source tool for malware analysis, suspicious html title, detection of phishing site, etc), where it attempts to trick users into entering their credentials.

The html file directs the user to a webpage with a fake/spoofed Hays logo as seen in the report to make it appear more legitimate, which could indicate a targeted phishing campaign against Hays and the recipients. However, this appears to be a low-risk campaign since no known malwares have been detected in the report to be running in the background and/or processes.

Kind regards,

Associate Security Analyst

HAYS Working for your tomorrow

Sydney, NSW,

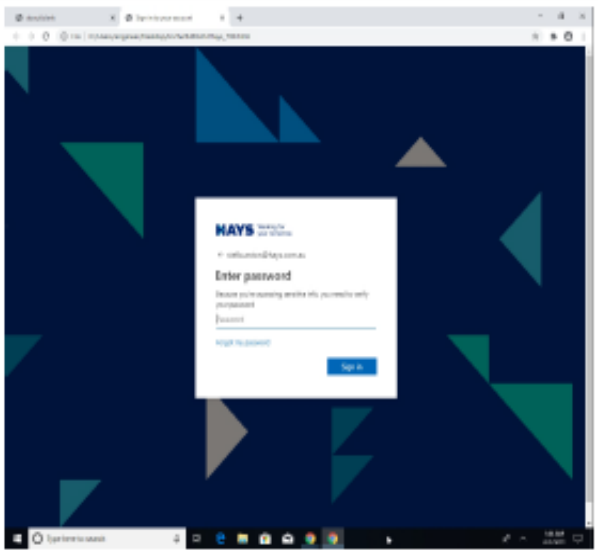
Connect with me on LinkedIn

hays.com.au | hays.net.nz

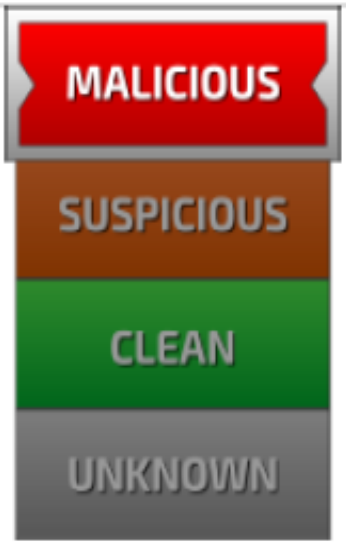
Overview

General Information

Sample Name:	Inv#[redacted]Hays_[redacted].html
Analysis ID:	[redacted]
MD5:	[redacted]ff6de7..
SHA1:	[redacted]db..
SHA256:	[redacted]de098..
Infos:	HTTP

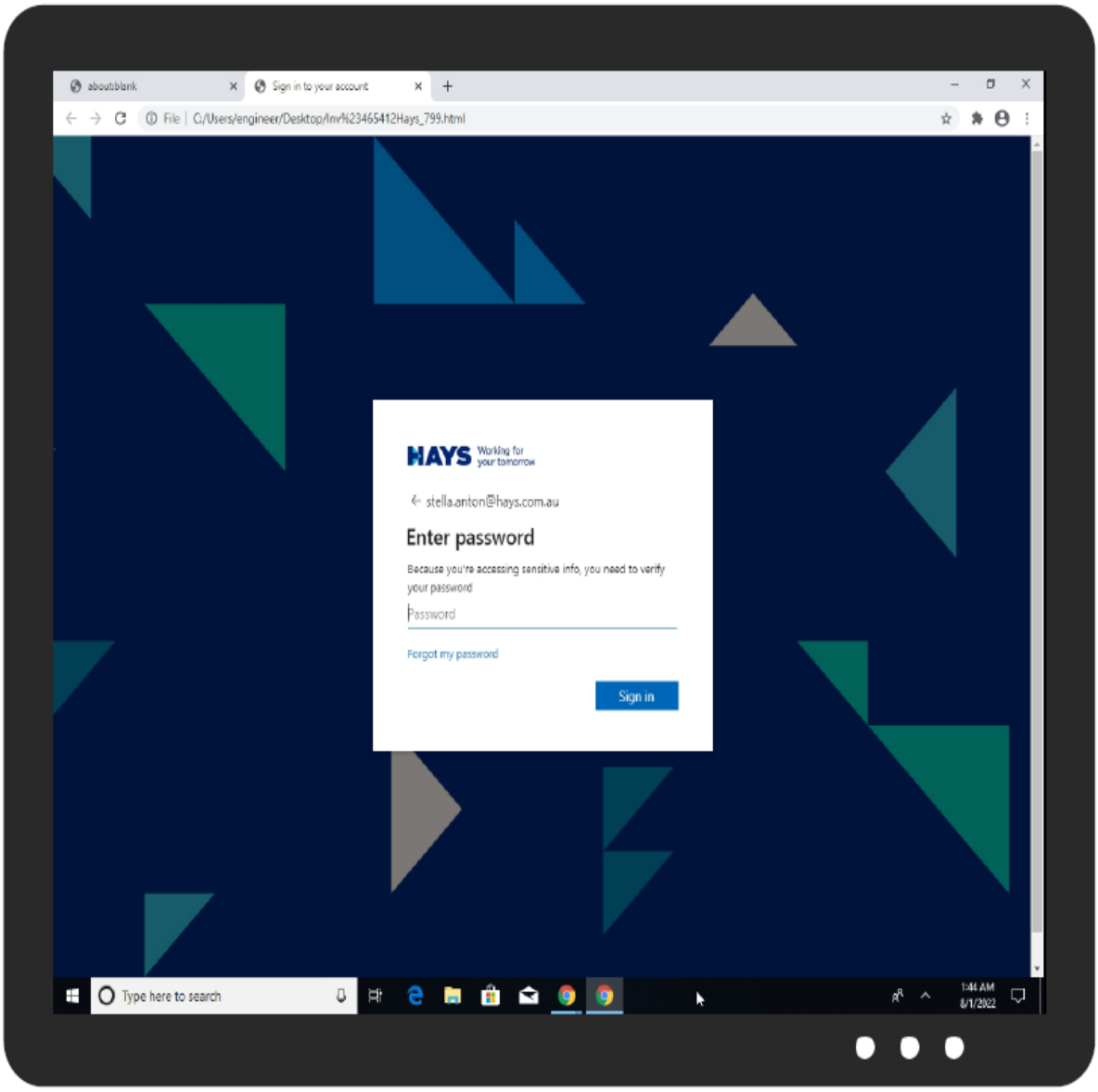


Detection



HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	[redacted]
Confidence:	100%



JoeSandbox Cloud BASIC

ID: [redacted]
Sample Name:
Inv#[redacted]html
Cookbook: default.jbs
Time: 01:43:41
Date: 01/08/2022
Version: 35.0.0 Citrine

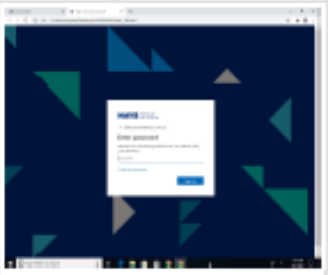
Windows Analysis Report

lnv#[redacted]html

Overview

General Information

Sample Name:	[redacted]
Analysis ID:	[redacted]
MD5:	[redacted]
SHA1:	[redacted]
SHA256:	[redacted]
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	[redacted]
Confidence:	100%

Signatures

[redacted]
HTML document with suspicious title
Phishing site detected (based on im....
JA3 SSL [redacted] in co....
HTML bo[redacted]ber of ....
IP addres[redacted] with ....
None HT[redacted]sensitiv...
No HTML[redacted]

Classification

Process Tree

- System is w10x64
- chrome.exe [redacted]
  - chrome.[redacted]
  - handle=1600[redacted]
  - handle=1944[redacted]
- chrome.exe [redacted]
- C139654B5C143[redacted]
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
[redacted]ages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	[redacted]	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

[redacted]

Phishing site detected (based on image similarity)

System Summary

HTML document with suspicious title

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

Behavior Graph

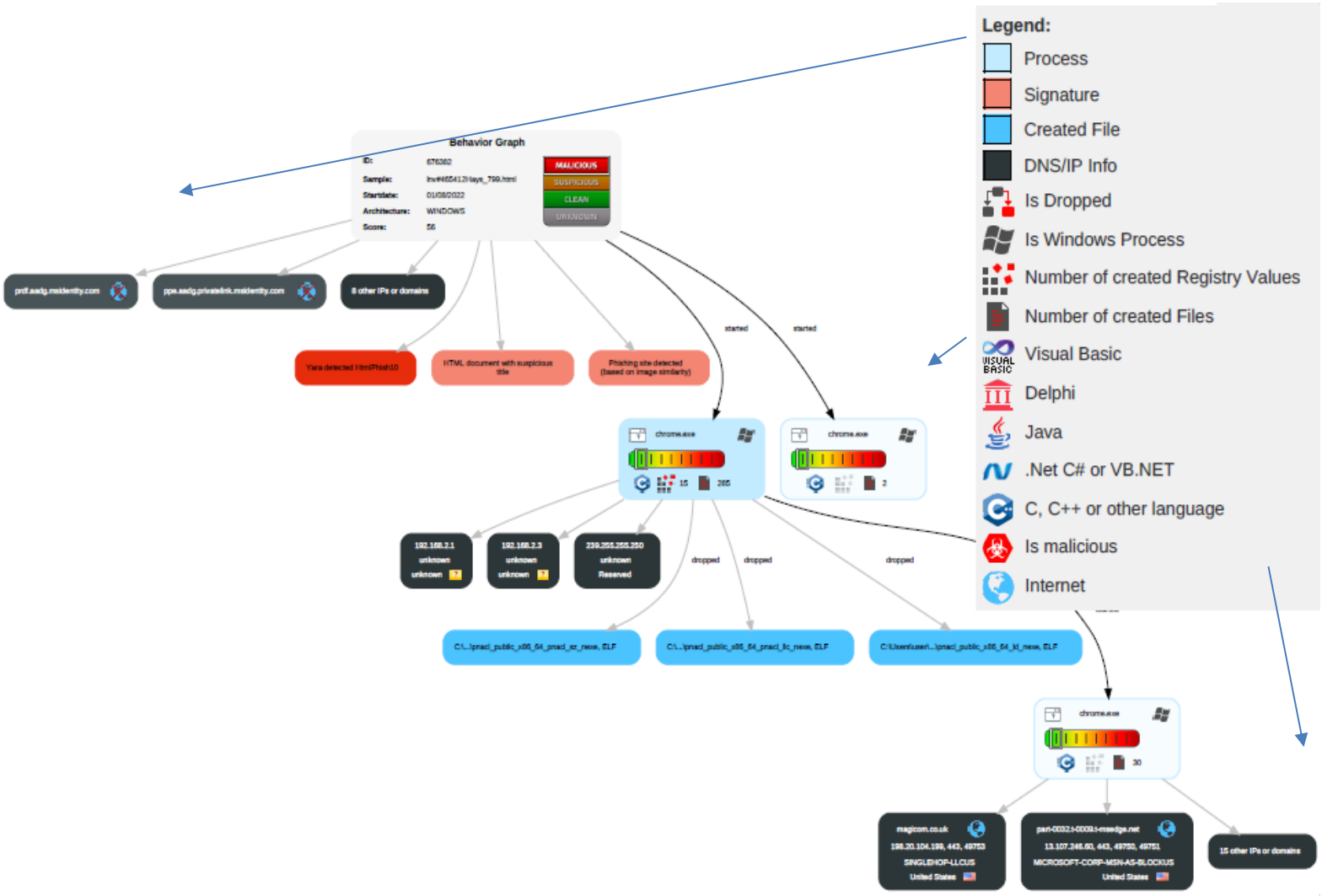


Figure: 04 – This diagram is mentioned above in Primary Methodology, and I have taken it from my own module and own drowning at Coventry University with Dr. Leon Smalov, which was **7033CEM** – "Information Security Risk Assessment for ABC Air" and submitted the LAST term.

The document is given below:

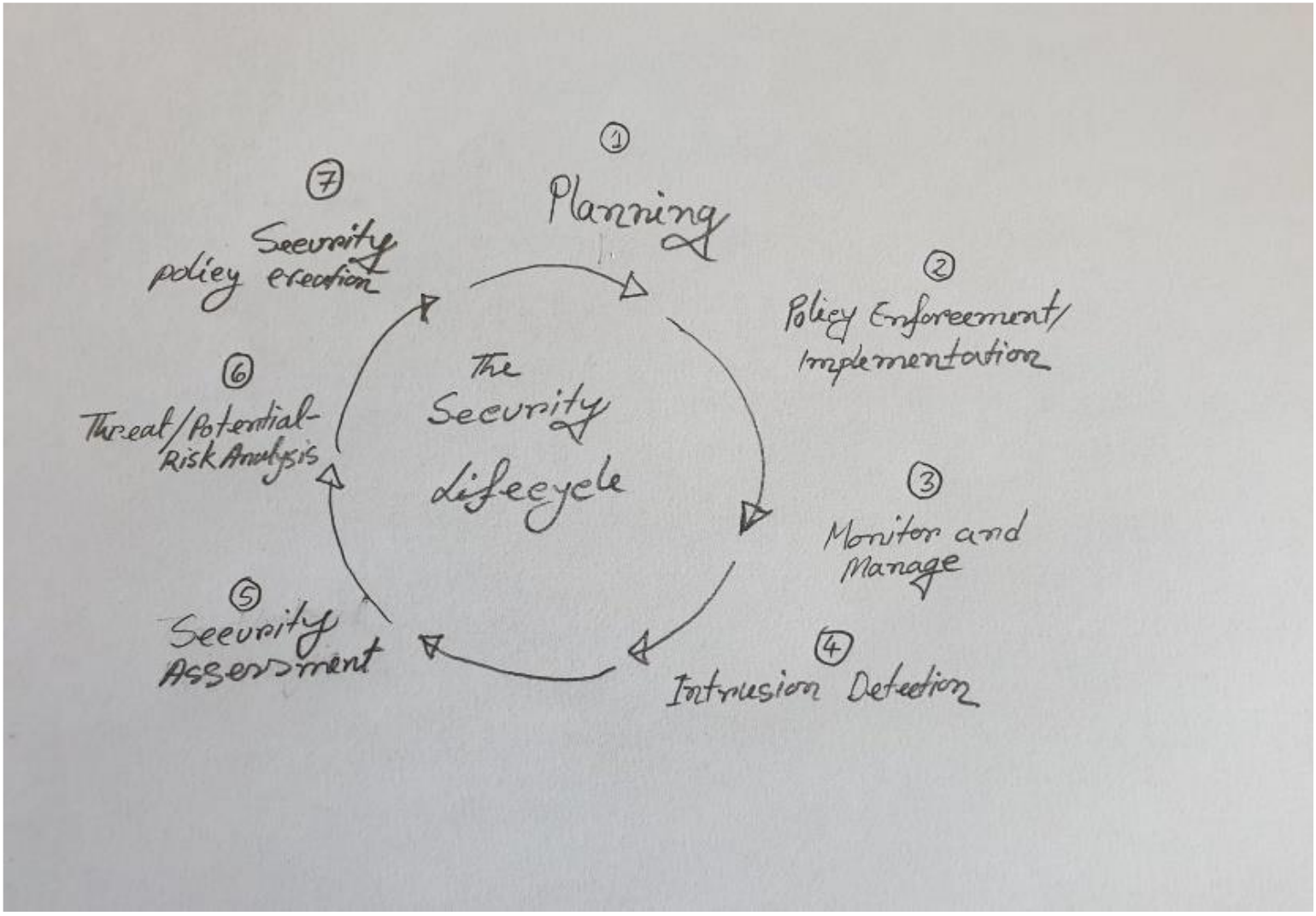


Figure: 05 - This document is above in this Project **in Paragraphs 5** (Only for explanation and Primary Methodology) and **Paragraph 6** (Secondary Methodology), and the whole document is extracted from Hays's ISMS Policy.

However, this is 16 pages document but given a few of them to understand how is the "ISMS Policy" and how the ISMS team Implements and Enforces based on this. Black masks cover data and Information due to GDPR and Hays's Commercial Confidentiality Policy. These documents are given below:

1. Executive Summary

For Hays, the information it possesses is one of its most important assets. For this reason, it is crucial that all information must be classified, accurate and available in order to meet the business needs of the company.

Guided by the standards set [redacted] nce that Hays employees protect company [redacted] ust, therefore, be made aware of the need [redacted] reserve these standards. Only by protecting [redacted] its civil and legislative legal obligations.

This document makes reference to the minimum information security policies that must be implemented in order to achieve information security. This must be followed by all Hays employees (permanent employees and temporary staff on contract) in all Countries.

[redacted] nformation security measures, based on the value [redacted] s if security is lost, a Security Information Policies [redacted] and mechanisms to define the security objectives [redacted] nformation assets in accordance with business objectives and goals.

The policies must be subject to regular reviews, in order to keep aligned with any business, legal or legislative changes.

The responsibility for the enforcement of these policies lies with the local management of each business unit and branch, and any queries must to be addressed to the Information Security Officer.

In general, the Hays information security strategy must follow the ISO 17799, BS 7799 and ISO 27001 standards where possible.

2. Purpose

[redacted] ument is to provide an overall view and motivation for Hays employees to [redacted] r a proper Information Security framework. This will apply to all IT related [redacted] n the company.

All regulations of this policy framework must be implemented in compliance with the applicable law and legal requirements.

This document defines the minimal mandatory requirements for the use of Hays information, and applies to all business processes.

Information must be protected in such a way that all legal and contractual obligations of Hays businesses can be fulfilled and add value for our customers.

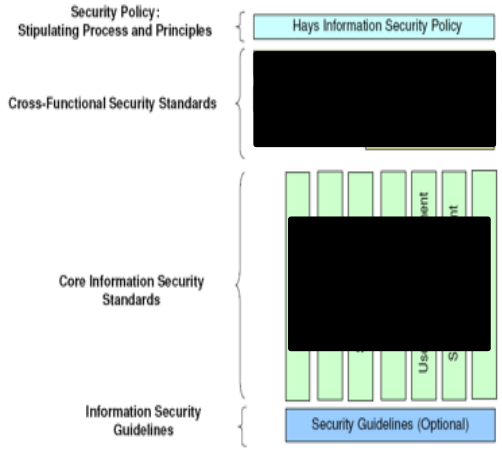
The objective of information security is to ensure:

[redacted]

Integrity:
Protection against any kind of modification, reproduction or storage, including any kind of service or resources manipulation that has not been authorised.

Availability:
Ensuring that all business significant information and services are available when required, to authorised users or processes.

No-repudiation:
Ensuring that information can be proven to have originated from an alleged individual, enterprise or process.



The above diagram represents the layers of the information security framework, which is summarised in the following standards.

Security Policy:
The present document states the principles and philosophy of the security policy that applies to all Hays employees, contractors and third parties, in a mandatory way.

[redacted] framework, across [redacted] ess, processes, [redacted] tomatic), and applies [redacted].

[redacted], which provide the m[redacted] ecifications, across the [redacted] ocesses and procedures [redacted].

[redacted] describe the minimum requirements demanded by Hays, stipulate the principles that apply in the context of IT security, and need to be followed and contractors.

3. Scope

This will apply to all information that is created, received, stored, processed, transmitted or printed using any system or storage medium, including information that is stored in any cloud-based environment used by Hays.

This will apply to all Hays employees and branches as well other individuals who directly or indirectly use or support the business system, infrastructure or information of Hays.

4. Hays Information Security Standards and Policies

The Hays Information Security Standards and Policies are a suite of documents as listed below.

- [redacted]

5. Roles and Responsibilities

[redacted]s in an

[redacted]
security.

5.1 Owner of the security policy

[redacted] document).
[redacted]mentation to
[redacted] Information
[redacted]gned by the
Production [redacted].

5.2 Production S[redacted]

- [redacted]plementation, and maintenance of Hays UK wide strategic
- [redacted]ementation, and enforcement of information systems security [redacted] guidelines, operating procedures, and technical standards

- Oversees the process of handling requested policy exceptions.
- Advise the Management Board on related risk issues and recommend appropriate actions to minimise any identified risks.
- Ensure related compliance requirements are addressed, e.g. security, and administrative regulations associated with federal and state laws.
- Ensure appropriate risk mitigation and control processes for security are implemented.

5.3 [redacted]

- [redacted]s Director on all security related matters on a regular basis
- [redacted]curity policies, procedures, standards and guidelines.
- [redacted]essment and advise suitable remedial action.

5.4 System owners

- The system owner should define which users or user groups are allowed access to the information and what authorized use of this information consists of.
- The system owner in consultation with the IT department, is responsible for purchasing requirements, development and maintenance of information and related information systems.

5.5 [redacted]

- [redacted]rsons administering Hays information systems and the information [redacted]arties
- [redacted] system may have one or more dedicated system administrators. [redacted]ible for protecting the information, including implementing systems [redacted]ard confidentiality, and carry out backup procedures to ensure [redacted]on.
- [redacted] run and maintain the security systems in accordance with the security policy

5.6 Business Directors and Managers

Business Managers and Directors are persons leading a team, [redacted]n, who will

- [redacted]ation security policies, procedures, cont[redacted]ntermeasures [redacted]ormation security program that comprise[redacted]eir day-to-day [redacted]r supervision are implemented.
- [redacted] staff, the appropriate security controls [redacted]esponding to [redacted]cation.
- [redacted]s within their areas of responsibility take[redacted]o comply with [redacted]Managing Director or Management Boa[redacted]mpact of any [redacted]t or respond to a security incident.
- [redacted]uccessfully complete any information s[redacted]training when
- [redacted]the IT Department, keep track of operati[redacted]which Hays is
- [redacted]emoval of access is lodged for users who[redacted]cess

5.7 Users

Users are persons who access and process Hays information and information systems in order to perform their day to day responsibilities. Users will

- [redacted]cedures, and control techniques identified in the Hays Information [redacted]ures and Standards.
- [redacted]y notifications sent by the IT department to mitigate the impact of any [redacted]espond to a security incident.
- [redacted]ected information security incidents and violations to the Hays Service [redacted]d entities.
- [redacted]ormation security awareness training as and when required.

5.8 [redacted]

- [redacted]ent prior to accessing [redacted] ensuring that this is implemented.
- Adhere to policies and process about external access.

6. Security Policy Change Management Procedure

All IT security management policies and standards must follow the following steps when they are created and/or modified:

- [redacted]
- [redacted]ment review/Board of directors (if a major change is nominated)
- [redacted]
- [redacted]
- [redacted]missing
- [redacted]

7. Enforcement

All Hays employees and contractors will be required to agree with the terms of this policy and any violation of these Security policies and standards could lead to disciplinary action and possible dismissal.

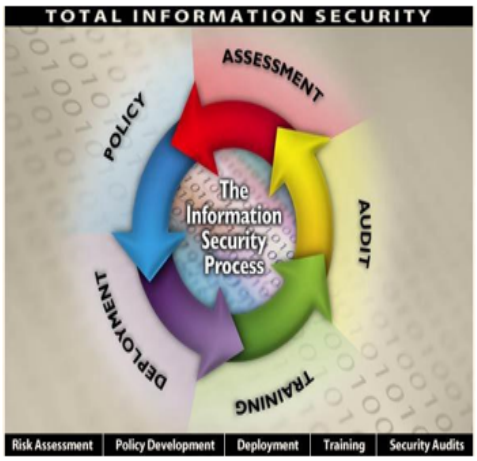
8. Information Security Management

All Hays employees need to understand the objectives of the information security policies Therefore, to achieve these objectives it is essential that:

- [redacted]chanisms to protect the asset values in association
- [redacted] in place for those systems that support business [redacted]with enough detail to identify unauthorised access or [redacted] systems.
- [redacted]on the business systems, to check the administration
- [redacted]d measures to protect the systems which handle
- [redacted]rrect use and handling of information
- Make all Hays employees aware of how to handle and maintain the information securely during this engagement with the company, during work time and out of hours
- Make leavers aware of their legal responsibility not to disclose any information handled while in employment, after his/her employment (or contract) ceases.

8.1 Information Security Life Cycle

The Information security life cycle is shown in the following diagram and explained in detail within this document.



Source: www.fortrex.com

8.2 [redacted]

As part[redacted]it is important to analyse and classify the risks associated with the various[redacted]ys' Information Systems (IT systems, processes, procedures, informa[redacted]

The res[redacted]is will classify the priority and p[redacted]sks. This will be [redacted]wed in order to provide recomm[redacted]minimize these ri[redacted]

Any ris[redacted]essed within specific controls must be brought to the attention of senior [redacted]risks for further analysis.

An Info[redacted] be appointed for every significant item or class of information, applica[redacted]structure component.

By cons[redacted]sociated with a loss of confidentiality, a[redacted]ty and non-repudia[redacted]ss, the owner must assign an appropria[redacted]ation.

As a re[redacted] the cross-functional security standards can be applied.

8.3 Data Classification

<u>Figure: 06</u> - This document is above in this Project **in Paragraph 6** (Secondary Methodology), ***Conceptual Part***, which falls under **ISMS sub-branches**, and the whole document is extracted from Hays's ISMS Policy. See below:

However, this is 9 pages document but given a few of them to understand what the "SOC Policy" is and how the ISMS and SOC teams Implements and Enforce the team Enforce based on this and ISMS Policies Black masks cover data and Information due to GDPR and Hays's Commercial Confidentiality Policy. These documents are given below:

Hays's Cyber Security Manager and Information Security Officer sit together:

Document Information

[redacted]

Version number	Version 0.6
Document status	Sixth Draft

Document History

Version	Change	Author	Date
0.1	First Draft	[redacted]	10-Jan-2020
0.2	Incorporated changes suggested by Nigel and Sacha		24-July-2020
0.3	Incorporated Changes suggested by Deepesh		10-August-2020
0.4	Process Format changes		17-August-2020
0.5	CIP Changes - 2021 First Half		08-03-2021
0.6	CIP Changes - 2022		31-01-2022

Document Reviewer

Version	Name	Title	Date Reviewed
0.6	[redacted]	Head - IT Support, Production Services, SOC & ISMS	
0.6		Information Security Officer	
0.6		Technical Environment Manager	

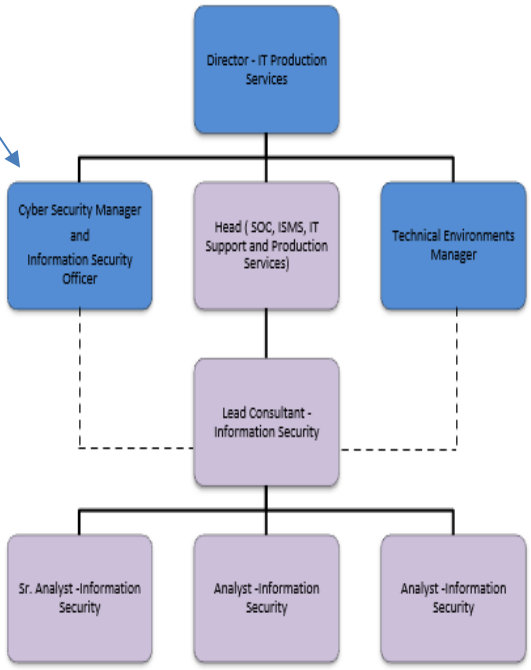
1. Introduction

This document describes the services delivered to Hays by the Security Operation Centre at Hays Business Solution.

2. Purpose

The SOC at Hays Business Solution strives to monitor and improve Hays IT infrastructure security posture continuously by detecting, preventing, analysing, and responding to cybersecurity threats using existing technology solutions and with strong set of processes.

3. SOC Organizational Chart



HAYS Recruiting experts worldwide

4. Terms and Definitions

4.1. SEP Client – [redacted] int Protection is an Antivirus installed on host

4.2. SEPM – [redacted] int Protection Management console used to client centrally

4.3. MSP – [redacted]

4.4. MSSP – [redacted] Provider

4.5. Resolver Team – [redacted] Hays support teams who work on resolving

4.6. Internal Stakeholders – [redacted] s internal teams like DIS, Marketing, Back office

4.7. RACI Matrix – [redacted] ective means for defining and documenting sibilities. It helps easily understand exactly who ountable, who needs to be consulted, and who every step will significantly improve your s. Please note Individuals can perform more than en required.

HAYS Recruiting experts worldwide

5. Process

5.1 Vulnerability Management						
Description	The purpose of Vulnerability management process is to detect and remediate and/or mitigate IT vulnerabilities in Hays environment timely.					
Process Ownership	Technical Environments Manager					
Scope & Task list	1. **Quarterly Internal Vulnerability Assessment** – This assessment is carried out on [redacted] using scanner placed within the Hays environment. This mainly [redacted] Assets at [redacted] This Assessment may cover Hays IT Assets in other regions as required. [redacted] erforms the assessment and shares report of discovered vulnerabilities [redacted] SOC upon receiving the report coordinates with the respective Internal Stakeholders in accordance with the internal vulnerability management procedure. 2. [redacted] part of Hays sets having public IP rk. The vendor performs ities with Hays ISO. [redacted] abilities with Critical and rnal stakeholders in [redacted] 3. [redacted] ype of assessments is carried accessible over the assessment and shares report [redacted] ulnerabilities with Critical and ys internal stakeholders in [redacted] edure. 4. [redacted] dition to the above-mentioned gement and/or Internal stakeholders n house vulnerability scanner and on team on the identified vulnerabilities in [redacted] g procedure. In addition to the above SOC is also responsible for maintaining the exception list as requested by the system owner and approved by Hays management.					
RACI Matrix	Analyst	IS Consultant	Technical Environments Manager	Head IT (Support, Production Services, SOC & ISMS)	Hays ISO	* Internal Stakeholders, Resolver Team, Computacenter
	R	R & A	C	I	I	C

Figure 07 – This document is above in this Project in **Paragraph 6.2 Practical** (Secondary Methodology), and the whole document was extracted from Technology Law Advisory – CRET Regulation, 2022 main document.

However, this is 3 pages document but given the 1st page of it to understand how the "new law" is and how the ISMS team Implemented and Enforces based on this and changed Hays's IRM process. Black masks cover data and Information due to GDPR and Hays's Commercial Confidentiality Policy. The document is given below:

KOCHHAR&CO.
ADVOCATES & LEGAL CONSULTANTS

Technology Law Advisory – CERT Regulations, 2022

INTRODUCTION

On April 28, 2022, the Indian Computer Emergency Response Team ("CERT") which is part of the Ministry of Electronics and Information Technology issued directions ("Direction") under Section 70B of the Information Technology Act, 2000 relating to reporting of cyber security incidents. This client update summarizes the requirement under the law and analyses the implications of the same.

BACKGROUND

The CERT was set up some years back to function as the nodal agency in the area of cyber security. It's powers include the collection, analysis and dissemination of information on cyber security incidents, providing forecasts and alerts, taking emergency measures and co-ordination of responses to cyber security incidents. It also has powers to issue directions to "service providers, intermediaries, data centres, and body corporates". Thereafter, certain rules were issued relating to CERT which also covered breach notification requirements. The rules were ambiguously worded and did not make clear that such notifications were mandatory. It related to cyber security incidents generally and was not related to breach of personal information of Indian citizens. Further, it did not address incidents that involved Indian businesses but where the concerned server was located outside India. It has therefore been a challenge to determine to what extent breach notifications were required in the case of global incidents with implications to Indian businesses.

AMBIT OF LATEST REGULATIONS

The scope of the Direction is extensive and quite unprecedented by global standards. The following are the key requirements:

1. ICT systems need to be synchronized with the network time protocol of the National Informatics Centre. In the case of international infrastructure, this can be done through other accurate and standard time sources.
2. Cyber security incidents are to be reported within 6 hours of noticing such incidents.
3. It would appear that in case an organization is subject to a cyber attack, it may receive directions from the CERT and would need to implement the same, failing which it would be treated as a non-compliance.
4. An organization needs to appoint a "Point of Contact" whose details need to be made known to CERT in a prescribed format. All CERT communications would be sent to the Point of Contact.
5. An organization needs to maintain logs of its ICT systems for a period of 180 days and also needs to maintain the logs within Indian jurisdiction.
6. Certain types of cloud and VPN providers need to obtain subscriber information and maintain the same for a period of 5 years. They also have to maintain information on IP addresses allotted or being used by subscribers.
7. Virtual asset providers and exchanges need to collect KYC information as per Indian regulations and maintain the same for a period of 5 years.

The Direction is troubling in many respects and is possibly the most disruptive regulation we have seen in the tech sector in India. We have analyzed below, some of the key issues:

ANALYSIS

Definitions

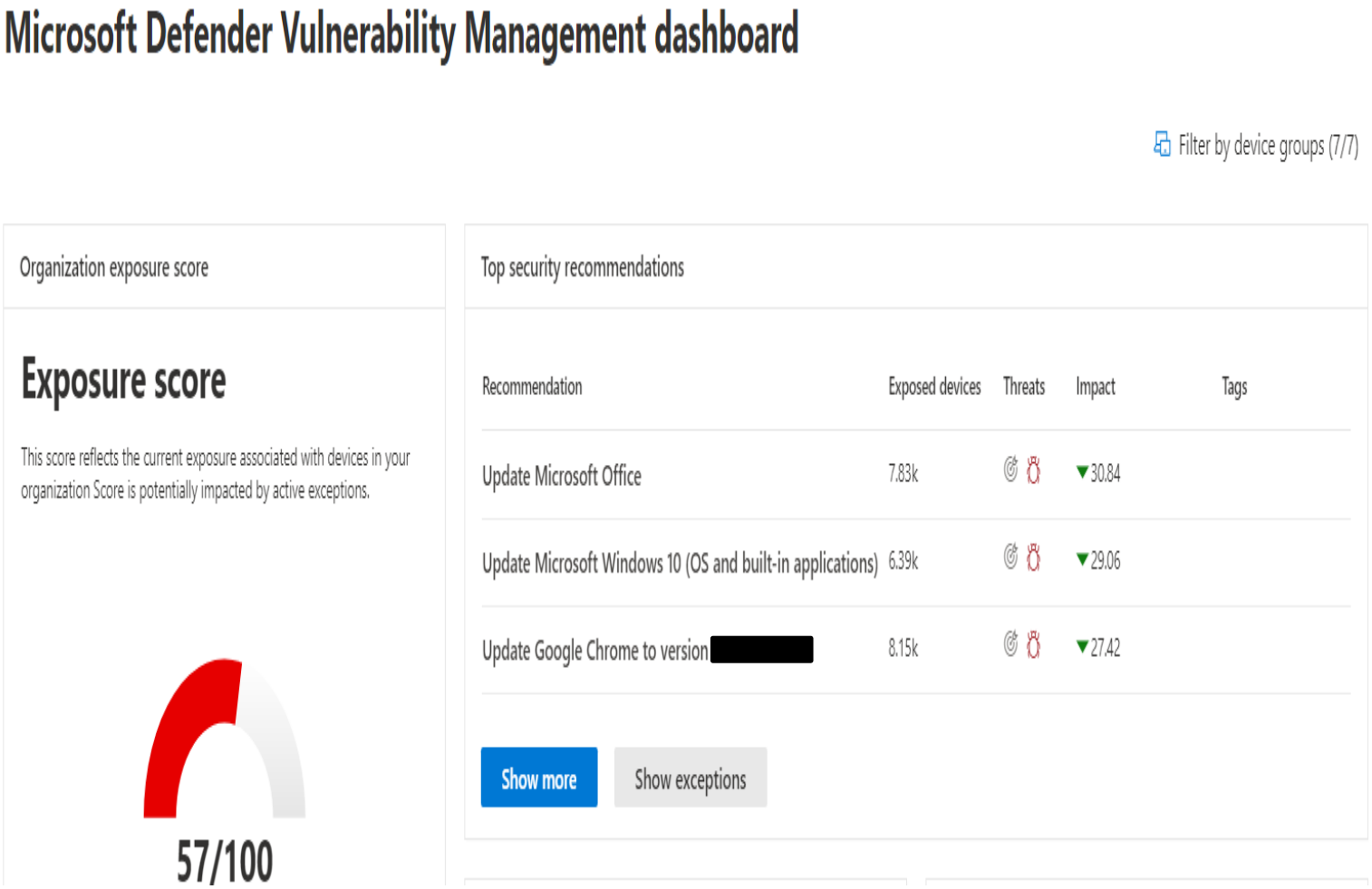
The regulations use general terms without defining clearly what those terms mean, thereby applying the regulations very broadly. For example, most of the Direction (other than that applicable to cloud providers and virtual asset providers) applies to "body corporates". In section 43A of the statute, a body corporate covers every kind of business, including partnership firms and sole proprietorships. This means it applies to every single business operating in India.

There is also reference to ICT systems with regard to maintaining logs. ICT in general parlance stands for information and communications technology. This covers all IT and communication systems.

Figure 08 - This document is referring to **Microsoft Defender (MS. D) in paragraph number 6.2.1**of this project for the **UK&I**, but the whole document is extracted from the **MS. Defender** tool utilised at Hays.

Microsoft Defender reports explained how to monitor End of Life Cycle (EOL), Vuln assessment, and managed by the CC for the EDR solutions and any record or evidence that the ISMS Governs other regions.

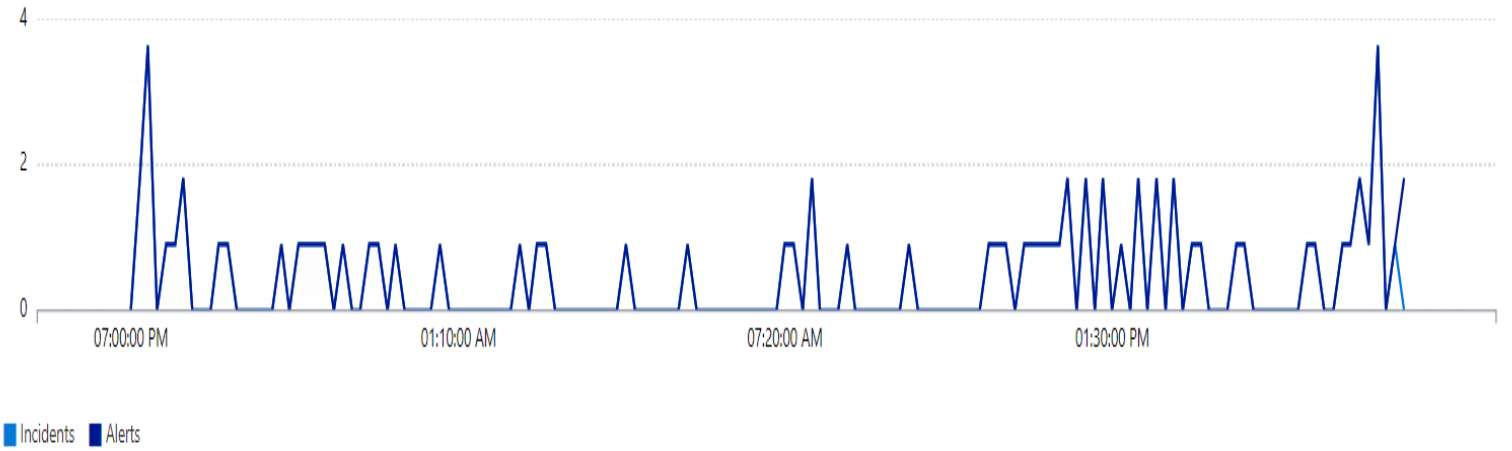
The full report is given below:



Incidents

Create a notification rule

Most recent incidents and alerts



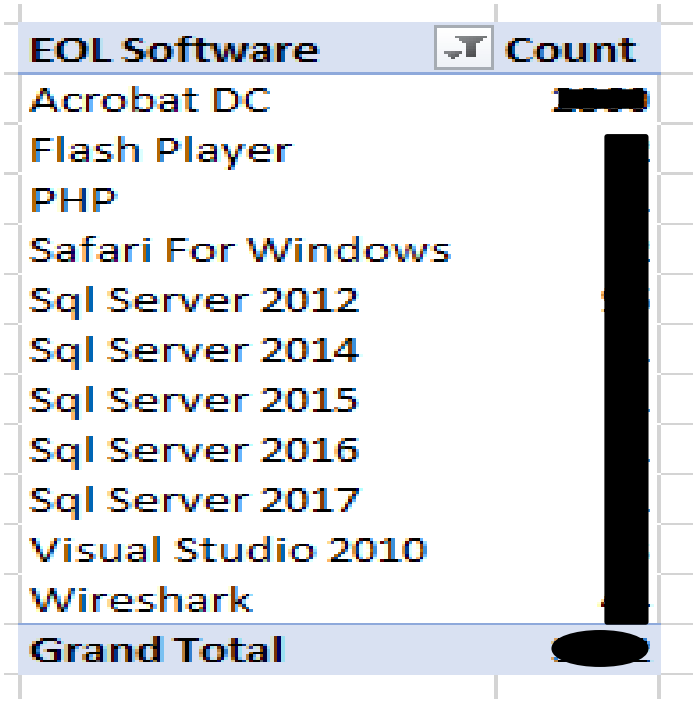
1-15 30 days Choose columns 30 items per page Filters

Incident name	Tags	Severity	Investigation state	Categories	Impacted entities
Persistence incident on one endpoint		Medium	2 investigation stat...	Persistence	[redacted].emea.hays.... [redacted]
'Rootkit' malware was detected on one endpoint		Informational...	N/A	Malware	[redacted]emea.hays.loc
Malware was detected in an iso disc image file on one endpoint		Informational...	N/A	Malware	[redacted]mea.hays.loc
'Agent' malware was prevented on one endpoint		Informational...	N/A	Malware	[redacted].hays.loc
'Deelae' malware was detected on one endpoint		Informational...	N/A	Malware	[redacted]63.emea.hays.loc

However, this Excel sheet report by **MS. Defender** is a very big report but given a few pages of it to understand its function and EDR solution which the SOC and CC can remediate based on these reports. Black masks cover data and Information to GDPR and Hays's Commercial Confidentiality Policy. These further documents are given below:

	A	B	C	D	E	F	G	H
1	Date	IP Address	Region	Hostname	Vulnerable Software	Vulnerability Title	Hays Rating	CVSSv2
01	19/11/2021	[redacted]67:7a37:d8f	UK & Ireland	lt[redacted]1w4	Acrobat DC	End of Life Software	High	7.8
02	19/11/2021	[redacted]a02:c7f:d4b0:5100:f	UK & Ireland	lt[redacted]2	Acrobat DC	End of Life Software	High	7.8
03	19/11/2021	[redacted]1	UK & Ireland	lt[redacted]2	Acrobat DC	End of Life Software	High	7.8
05	19/11/2021	[redacted]::74df:ea56:9f0b:2	UK & Ireland	l[redacted]b3	Acrobat DC	End of Life Software	High	7.8
06	19/11/2021	[redacted]:b702, ::1	UK & Ireland	[redacted]	Acrobat DC	End of Life Software	High	7.8

	I	J	K	L	M	N
	CVE	Vulnerability Description	Consequence	Data Collected	Recommended Solution	References
1	CVE-202[redacted]/E-2021-39842, CVE-2021-39843, C[redacted]844	Reported Software is End of Life	No Vendor support for End of Life Software	202[redacted]0	Users update their application with the newest version	[redacted]elpx.adobe.com/security/products/acrobat/aps[redacted]tml
2	CVE-202[redacted]/E-2021-39842, CVE-2021-39843, C[redacted]844	Reported Software is End of Life	No Vendor support for End of Life Software	202[redacted]0	Users update their application with the newest version	[redacted]elpx.adobe.com/security/products/acrobat/aps[redacted]tml
3	CVE-202[redacted]/E-2021-39842, CVE-2021-39843, C[redacted]844	Reported Software is End of Life	No Vendor support for End of Life Software	202[redacted]0	Users update their application with the newest version	[redacted]elpx.adobe.com/security/products/acrobat/aps[redacted]tml
5	CVE-202[redacted]/E-2021-39842, CVE-2021-39843, C[redacted]844	Reported Software is End of Life	No Vendor support for End of Life Software	202[redacted]0	Users update their application with the newest version	[redacted]elpx.adobe.com/security/products/acrobat/aps[redacted]tml
6	CVE-202[redacted]/E-2021-39842, CVE-2021-39843, C[redacted]844	Reported Software is End of Life	No Vendor support for End of Life Software	202[redacted]0	Users update their application with the newest version	[redacted]elpx.adobe.com/security/products/acrobat/aps[redacted]tml



EOL Software	Count
Acrobat DC	[redacted]
Flash Player	
PHP	
Safari For Windows	
Sql Server 2012	
Sql Server 2014	
Sql Server 2015	
Sql Server 2016	
Sql Server 2017	
Visual Studio 2010	
Wireshark	
Grand Total	[redacted]

Figure 09 and 10 - This document is referring to ***Browsing Plug-in Security Assessments*** (**Plug-In SA**) **in paragraph number 6.2.2** of this project for the **UK&I**, but the whole document is extracted from the **SOC** Assessments record at Hays.

This report explained how Browsing Plug-in Security Assessment conduct based on record/ docs/ evidence. The full report is given below:

HAYS Recruiting experts worldwide

SECURITY ASSESSMENT OF CHROME EXTENSION - GLOSSARYTECH

HAYS Recruiting experts worldwide

EXECUTIVE-SUMMARY

Extension Name:	[redacted]sion
Extension Description:	Glossary Tech is Google Chrome plugin which allows you to check technical terms used webpage in fast way
Execution Method:	Chrome automatically activates plugin and provide access to tabs and executes the plugin script on it.
External Connections:	29 URLS (Please refer to detail report)
Privacy Exposed in Data transmission	Few data transmission was found to be done over HTTP in clear text format.
External Emails founds	None
Permissions:	**Total – 2** • **cookies -** Access information about an HTTP cookie. • **tabs -** To interact with the browser's tab system and execute Script on tab when content match is found.
Background Script Execution:	**No**
Risk Classification	**Low**
Expected IMPACT	Plugin remains active on all webpage browsed in google chrome and store access HTTP cookie in user browser.
Report Summary	During the security [redacted] that the plugins has access to all tabs of [redacted] and use this access to read [redacted] ms in an overlay. This plugin uti[redacted] cookie (HTTP). [redacted] was requested or obtained by plugin [redacted] in line with its intended purpose

Security Assessment Report is given below:

Detailed Security Assessment Report

[redacted]_Detail
_Technical_report.xl

Name	GlossaryTech Chrome Extension
Version	0.10.4
URL	[redacted]ch-w/lkfaknngnekohfmljebdikgefjfhkgkp

Plugin Background Execution Check	
Persistent Execution	No
Scripts	[redacted].js, background.js, analytics.js

Content based Script Execution Check	
URLs	Scripts
https://*/*	[redacted]st-plugin-tooltip.js, main.js
http://*/*	[redacted]js, main.js

Permission	Yes/No	Remarks
activeTab	No	
declarativeContent	No	
system.storage	No	
alarms	No	
background	No	
fontSettings	No	
printerProvider	No	
browsingData	No	
clipboardRead	No	
gcm	No	
privacy	No	
tts	No	
unlimitedStorage	No	
identity	No	
storage	No	
contextMenus	No	
idle	No	
webRequest	No	
cookies	**Yes**	**Access information about an HTTP cookie.**
system.display	No	
webRequestBlocking	No	
system.memory	No	

Special Permssion	Yes/No	Remarks
notifications	No	
desktopCapture	No	
pageCapture	No	
tabCapture	No	
downloads	No	
tabs	**Yes**	**To interact with the browser's tab system and execute Script on tab when content match is found**
bookmarks	No	
topSites	No	
clipboardWrite	No	
power	No	
geolocation	No	
proxy	No	
ttsEngine	No	
history	No	
sessions	No	
contentSettings	No	
webNavigation	No	
system.cpu	No	
management	No	
debugger	No	
nativeMessaging	No	

The Last Part of the Assessment:

	A
6	https:/[redacted].mozilla.org/en-US/docs/Web/SVG/Element/foreignObject
7	http://[redacted]g/TR/SVG/extend.html
8	http://[redacted]g/TR/SVG/animate.html
9	http://[redacted]g/TR/SVG11/feature
0	http://[redacted]/Archives/Public/www-svg/2003Oct/0000.html
1	http://[redacted]me.io
2	http://[redacted]me.io/license
3	https:/[redacted]n
4	https:/[redacted]m
5	https:/[redacted]/license
6	http://[redacted]license
7	https:/[redacted]ch.com/auth/login?plugin=1
8	https:/[redacted].com
9	https:/[redacted].com/chrome
0	https:/[redacted]ch.com/scanner
1	https:/[redacted]e/employer

Figure 11 - This document is referring to **Pro-Active Monitoring of Hays's Asset by Splunk for the UK&I in paragraph number 6.2.3** of this project, but the whole document is extracted from the **Splunk** tool utilised at Hays.

> *Splunk is our direct Service Provider and a specialist from Splunk conducts training for our Security Personnel in order to implement all facilities from its original site, the main site could be found below:* Splunk | The Data Platform for the Hybrid World. (2022). Retrieved 31 July 2022, from https://www.splunk.com/

However, the full reports explained how Splunk conduct Pro-Active Monitoring at Hays. The full report is given below:

RSA audit - server logon without token

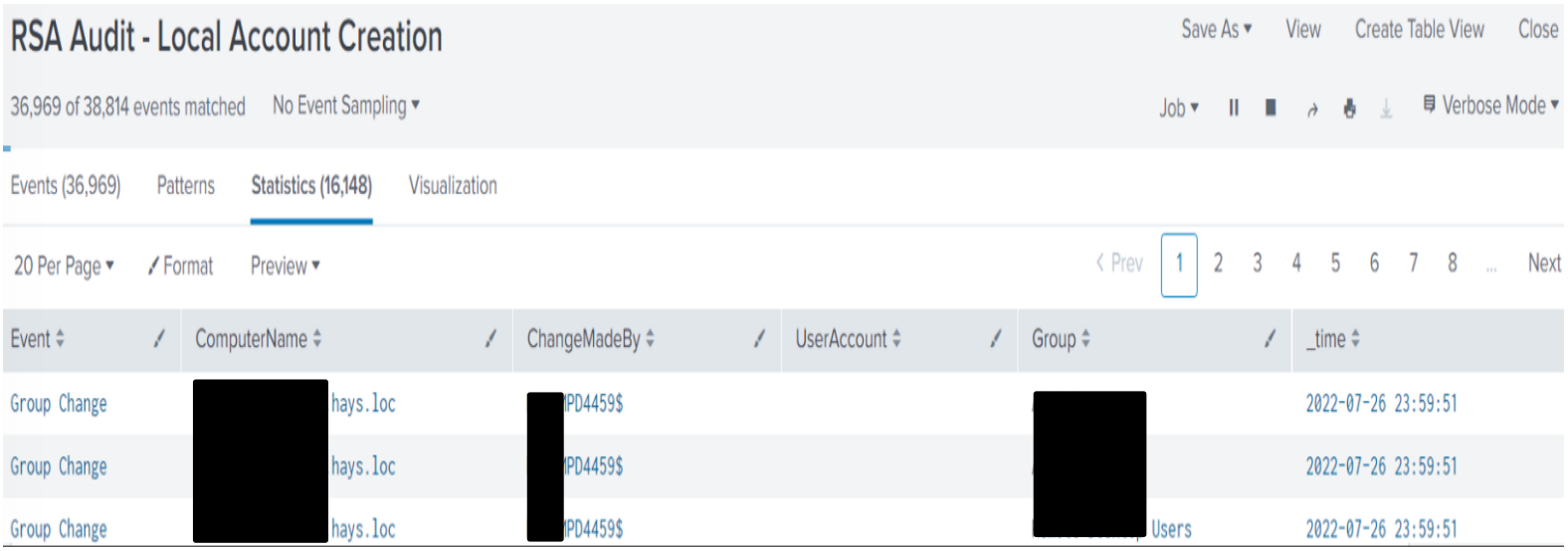
Save As ▾ View

✓ 186 events (26/07/2022 [redacted]0.000) No Event Sampling ▾ Job ▾

Events Patterns Statistics (186) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4

_time	host	SamAccountName
2022-07-26 21:00:54	[redacted]hays.loc	[redacted]BOT-PROD
2022-07-26 20:15:30	hays.loc	BOT-PROD
2022-07-26 20:00:52	hays.loc	BOT-PROD
2022-07-26 18:45:50	hays.loc	BOT-PROD
2022-07-26 16:23:01	hays.loc	
2022-07-26 16:22:44	hays.loc	
2022-07-26 16:00:36	hays.loc	BOT-PROD
2022-07-26 16:00:00	hays.loc	j
2022-07-26 15:47:23	hays.loc	
2022-07-26 15:04:26	hays.loc	BOT-PROD
2022-07-26 14:46:16	hays.loc	BOT-PROD
2022-07-26 14:15:09	hays.loc	BOT-PROD
2022-07-26 14:05:41	hays.loc	
2022-07-26 13:24:57	hays.loc	ics-support
2022-07-26 13:17:54	hays.loc	BOT-PROD



Splunk Dashboard report below:

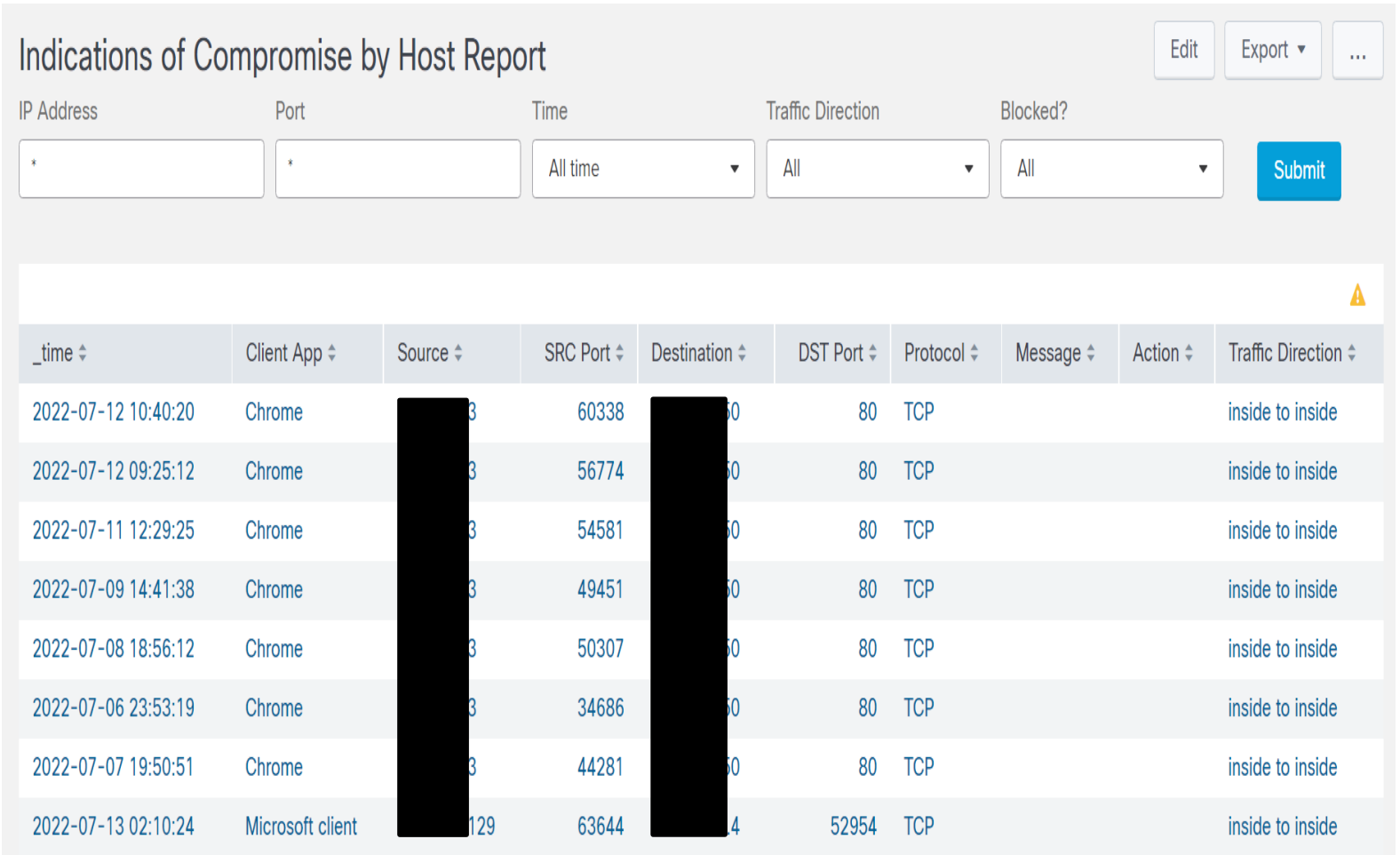
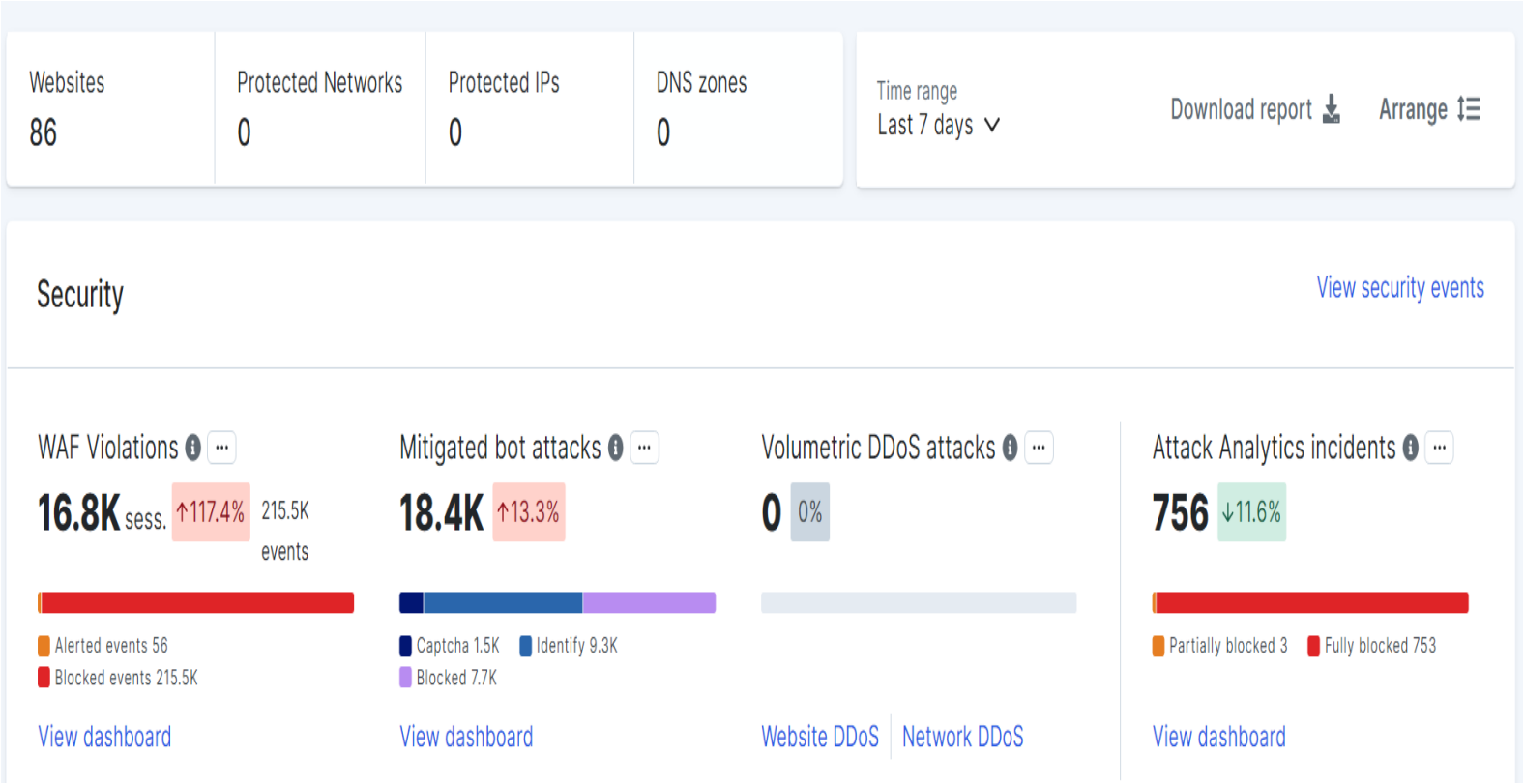
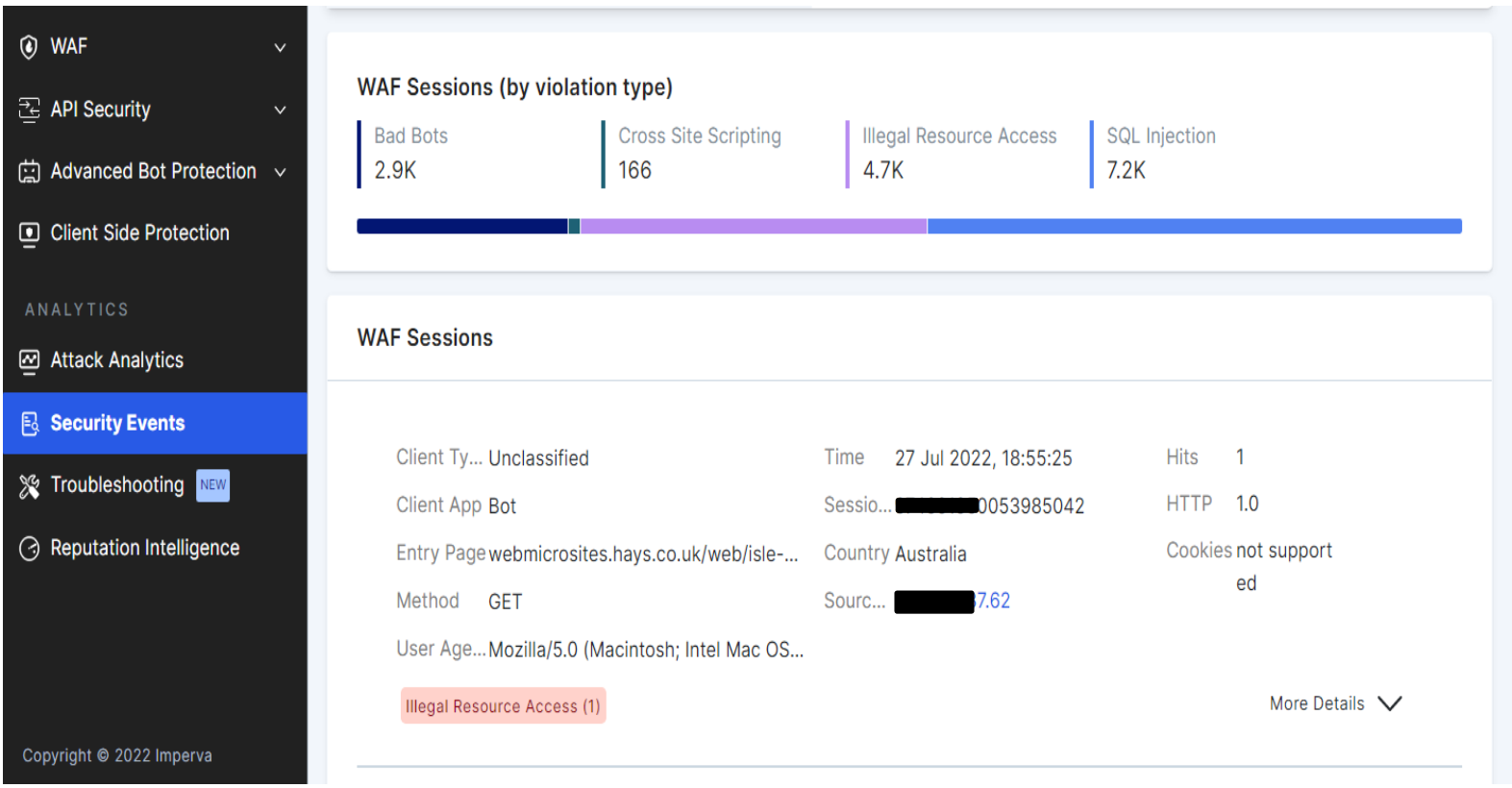


Figure 12 - This document is referring to **Web Application Firewall monitoring (WAF) for the UK&I in paragraph number 6.2.4** of this project, but the whole document is extracted from the **Imperva WAF** tool utilised at Hays.

However, the full reports explained how **Imperva WAF** conducts Web Application Firewall monitoring (as fine-tune, finetune rules, and others) at Hays. The full report is given below:





Imperva WAF Dashboard showed the whole picture for Web Application Firewall monitoring, Dashboard output is given below:

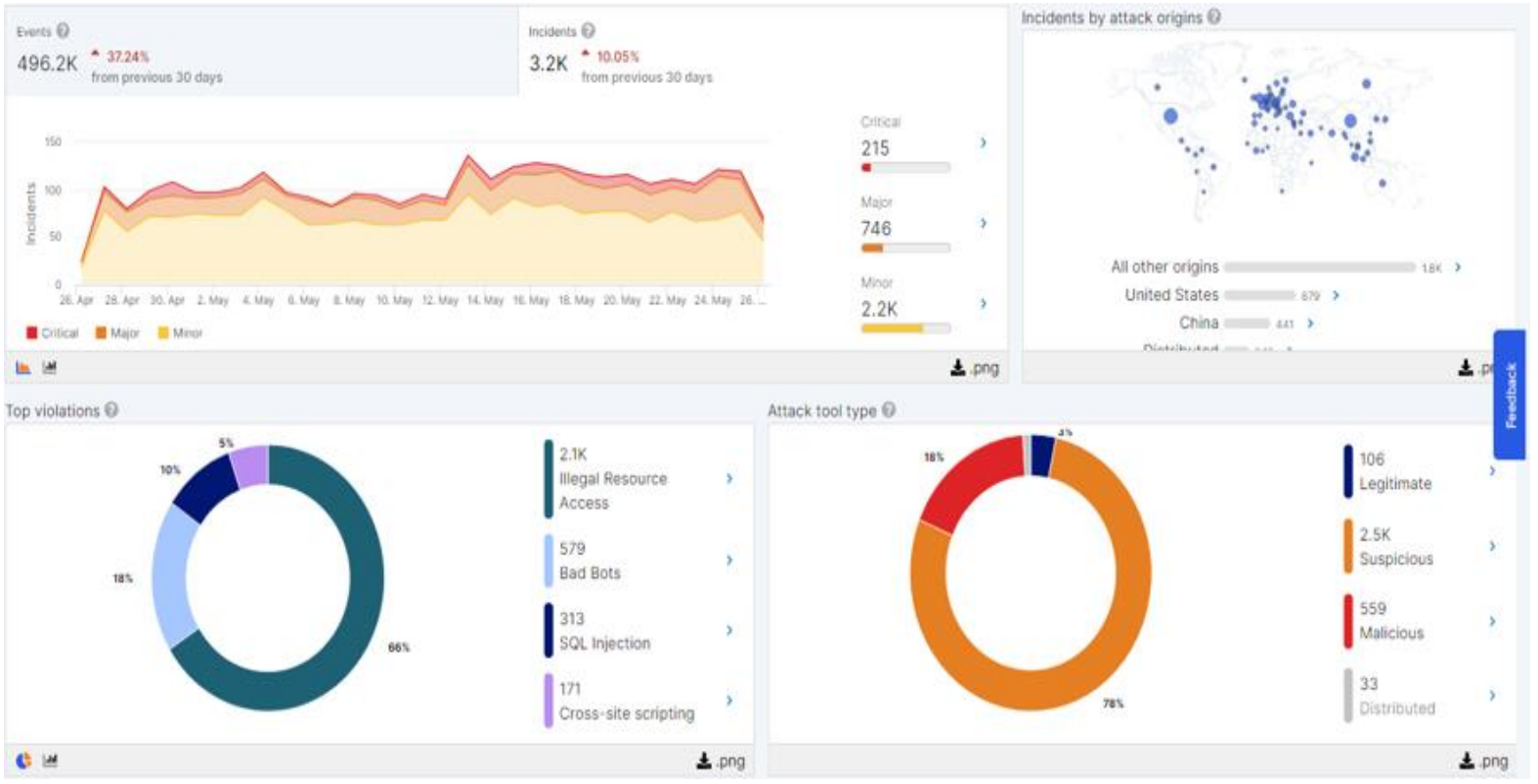
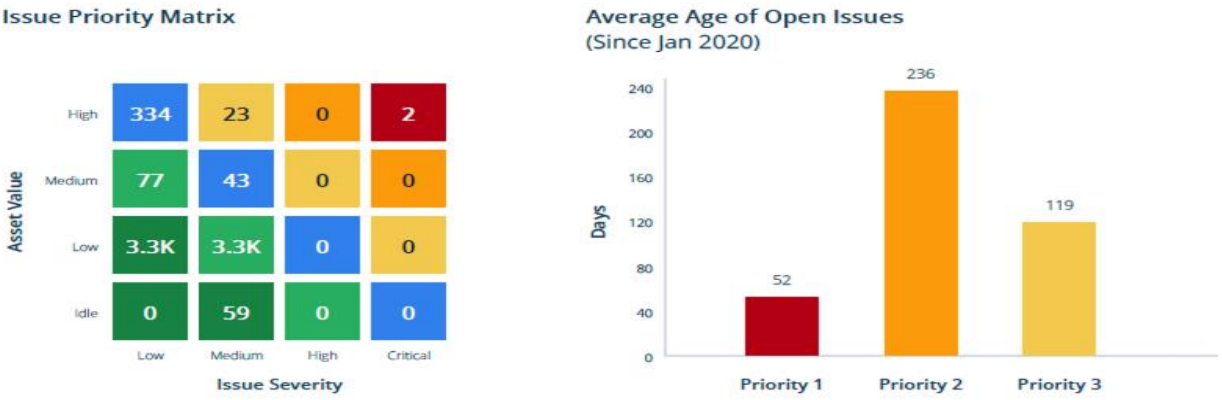


Figure 13 and 14 - This document is referring to the **3rd Party Risk Advisory for EMEA in paragraph number 6.2.5** of this project, but the whole document is extracted from the **3rd Party Risk Review** and utilised at Hays to reduce risks for Cloud Monitoring.

However, the full reports explained how the **3rd Party reviews the Risk** by utilising the tool at Hays's ISMS environments. The full report is given below:



Priority Matrix by RiskRecon for Cloud Monitoring (on above):

riskrecon mastercard

1 of 2

July 26, 2022

[redacted] Executive Report

[redacted]

RiskRecon monitors a company's web presence to determine their cybersecurity health rating on an A – F rating scale, with F being the lowest rating. Lower ratings correlate to higher breach event frequencies. B-rated companies average a 2x lower rate of breach events compared with F-rated companies.

RiskRecon Rating

B
7.5 / 10

Rating Range

Rating High

B 7.9

Rating Low

C 6.2

Breach Events (Over last 3 years)

No Event Occurences

Action Plan Summary

0	0	0	0
Total Issues Shared	Shared Issues Closed	New Issues Not Shared	Shared Issues Open

riskrecon mastercard

July 26, 2022

[redacted] Executive Report

Domain Ratings

Domain	Rating	Issues	Trend
Software Patching	A 9.9	1	0.0 →
Application Security	F 2.6	[redacted]	0.0 →
Web Encryption	D 5.4	[redacted]	0.0 →
Network Filtering	B 7.4	2	0.0 →
Breach Events	A 10	0	0.0 →
System Reputation	A 10	0	0.0 →
Email Security	A 8.5	7	0.0 →
DNS Security	A 10	4	0.0 →
System Hosting	B 7.8	0	[redacted]

Figure 15 - This document is referring to the **Office 365 (Security Monitoring) for the APAC in paragraph number 6.2.6** of this project, but the whole document is extracted from the **Office 365 tool (Auto Forward Messages)** and utilised at Hays to reduce risks for the Security Monitoring.

However, the full reports explained how **Office 365 (Security Monitoring)** utilises the tool at Hays's ISMS environments. The full report is given below:

Summary | New Activity

Auto forwarded messages

Monitor for potential data leaks when people in your organization automatically forward email messages to an external domain, such as a personal email address. Learn more

Forwarding type

Mailbox Rule

1 more

Recipient domain

16 more

Forwarding users

[redacted]m.au
[redacted]hays.com
[redacted]ays.com
[redacted]hays.pl

Auto forward message details

Office 365 Alert is given below:

Severity	Alert name	Status	Tags	Category	Activity cou...	Las
Informational	Creation of forwarding/redirect rule	Active	-	Threat management	1	
Informational	Creation of forwarding/redirect rule	Active	-	Threat management	1	
Informational	Creation of forwarding/redirect rule	Active	-	Threat management	1	
Informational	Creation of forwarding/redirect rule	Active	-	Threat management	1	
Informational	Creation of forwarding/redirect rule	Active	-	Threat management	1	
Informational	Creation of forwarding/redirect rule	Active	-	Threat management	1	
Informational	Creation of forwarding/redirect rule	Active	-	Threat management	1	

Figure 16 and 17 - This document is referring to the **Microsoft E5 Licence for Hays Global role in paragraph number 7.1** of this project, but the whole document is extracted from the **Microsoft E5 Licence** allocation tool and ongoing function at Hays for secure Hays Global Cyber and Information posture by this sophisticated tool.

However, the full reports explained its (**MS. E5 L**) **design, function, Compliance,** and **Implementation** in Hays's ISMS environments and capability. The full report is given below:

E5 Compliance

Information Protection and Governance

Microsoft Cloud App Security
Protect data in SaaS applications with, classification, encryption and UEBA to reduce risk of data loss

Teams chat and channel DLP
Block sensitive data from being shared in teams chats and channels.

Advanced Data Governance
Retain data based on sensitivity, and business events. Trigger disposition reviews.

Rules based auto classification
Automated classification and encryption for files on prem and in the cloud, based on sensitive data types

ML based auto classification
Trainable classifiers can learn about data types unique to your organization.

Advanced Message Encryption
Allow admins to revoke access to encrypted mails after delivery, and apply custom branding

Endpoint DLP
Prevent sensitive data upload to consumer cloud services, network shares, USB, printing etc.

Insider Risk Management

Insider Risk
Identify risk patterns by combining user HR info (e.g. Departing employees) with signals from DLP, classification labels, security policy violation, to generate insider risk events.

Communication Compliance
Detect harassment, offensive language & confidential project communications. Comply with regulations on appropriate messaging.

Information Barriers
Restrict communication and collaboration between groups/people to avoid a conflict of interest, or to protect internal data.

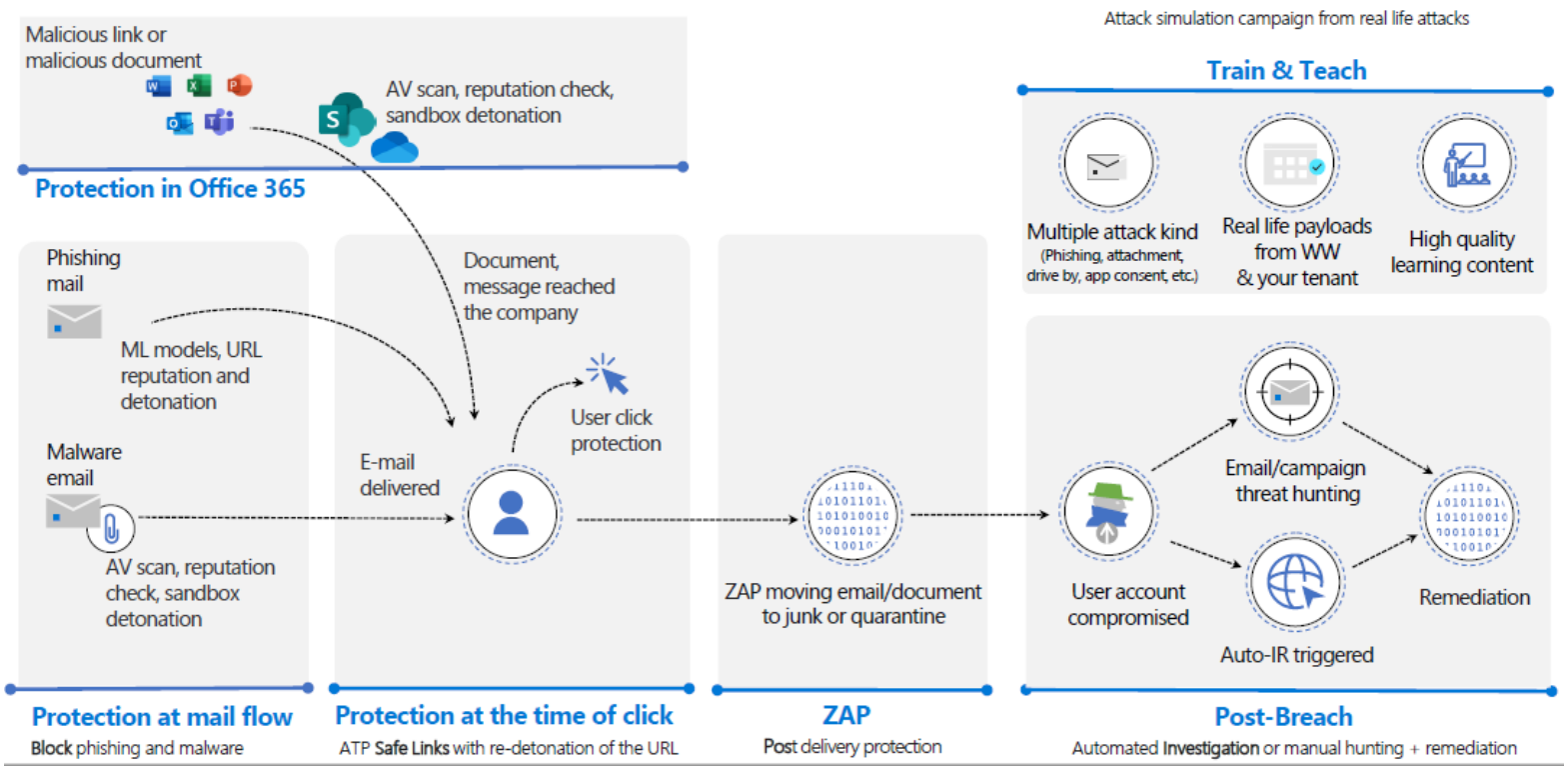
Privilege Access Management
Just in time access for M365 scoped at a task level.

Customer Lockbox
Ensures that Microsoft cannot access your content in M365 to perform a service operation without your explicit approval.

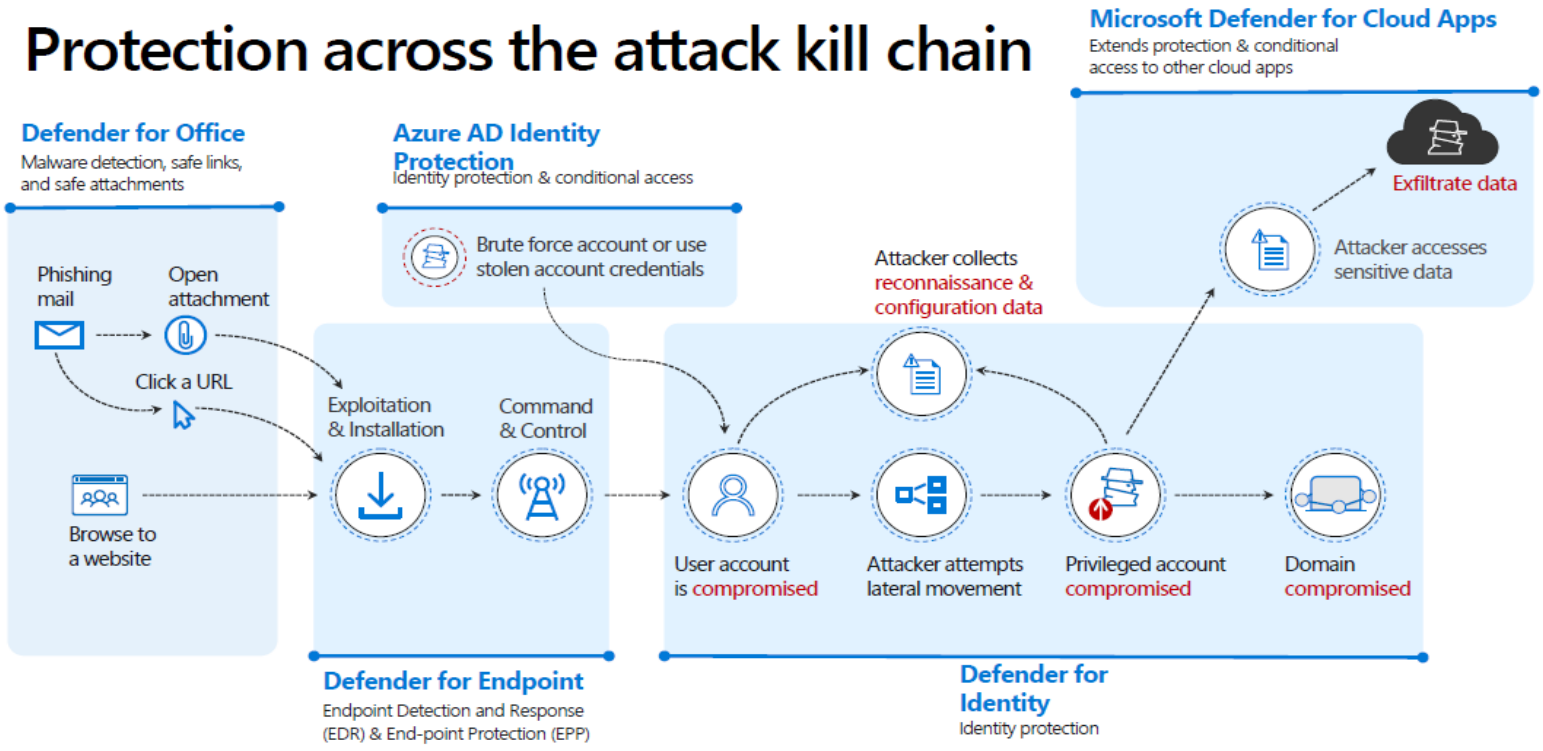
eDiscovery and Audit

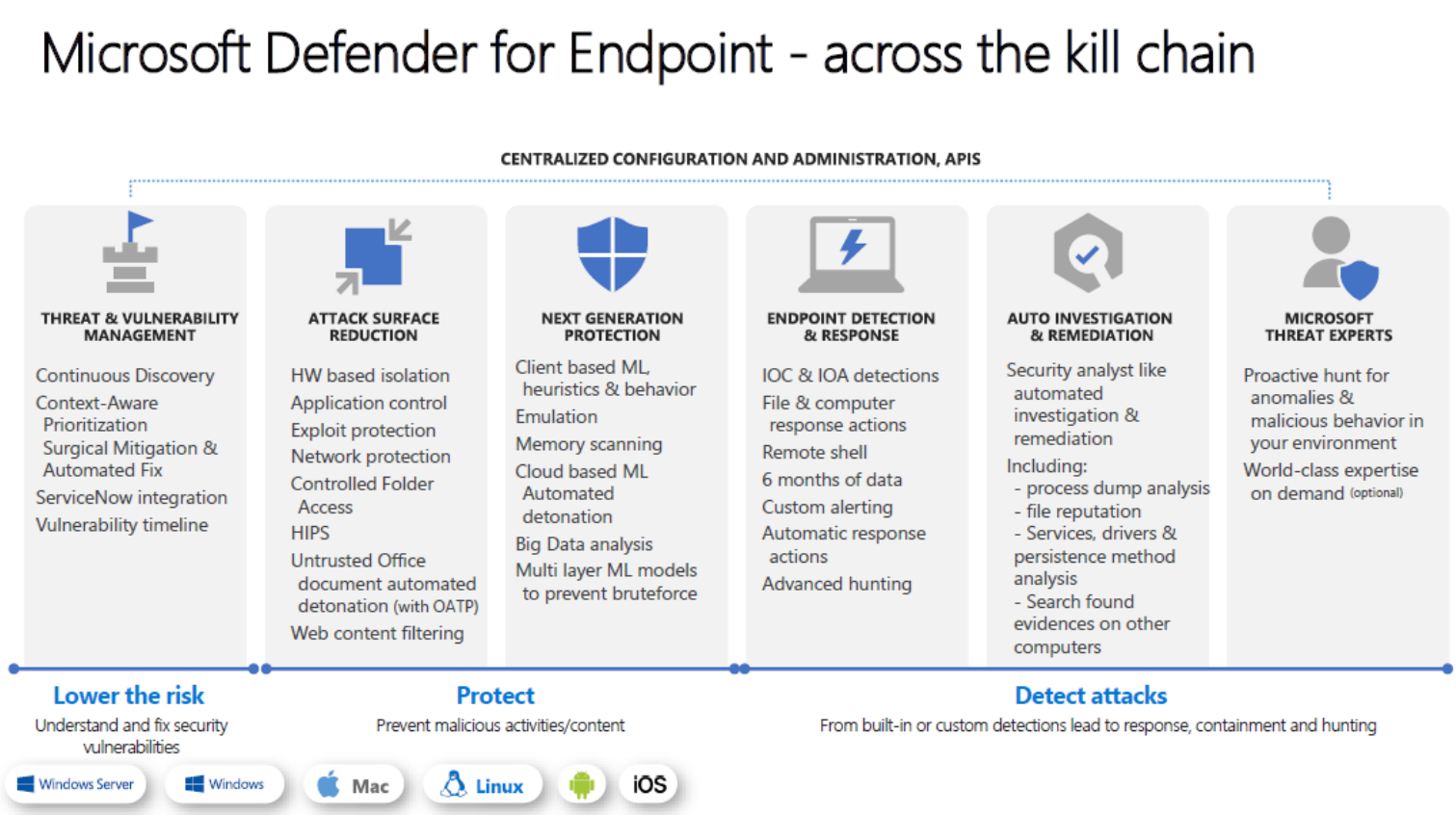
Advanced Ediscovery
Analyze and cull data intelligently with ML, Deeper indexing run in Azure cloud. Annotate and redact. Remove duplicates. Custodian management and comms. Together can reduce costs by 85%.

Advanced Audit
Audit log retention policies beyond the standard 90 days. Access to crucial events for investigations such as searching for accessed mailbox items.



This document was provided to Hays's ISMS team, as a part of the MS E5 License, which is a very big document, hence, I am providing a few of them to understand its reader about it, these documents are given below:





Cloud Security by MS. E5 L is given below:

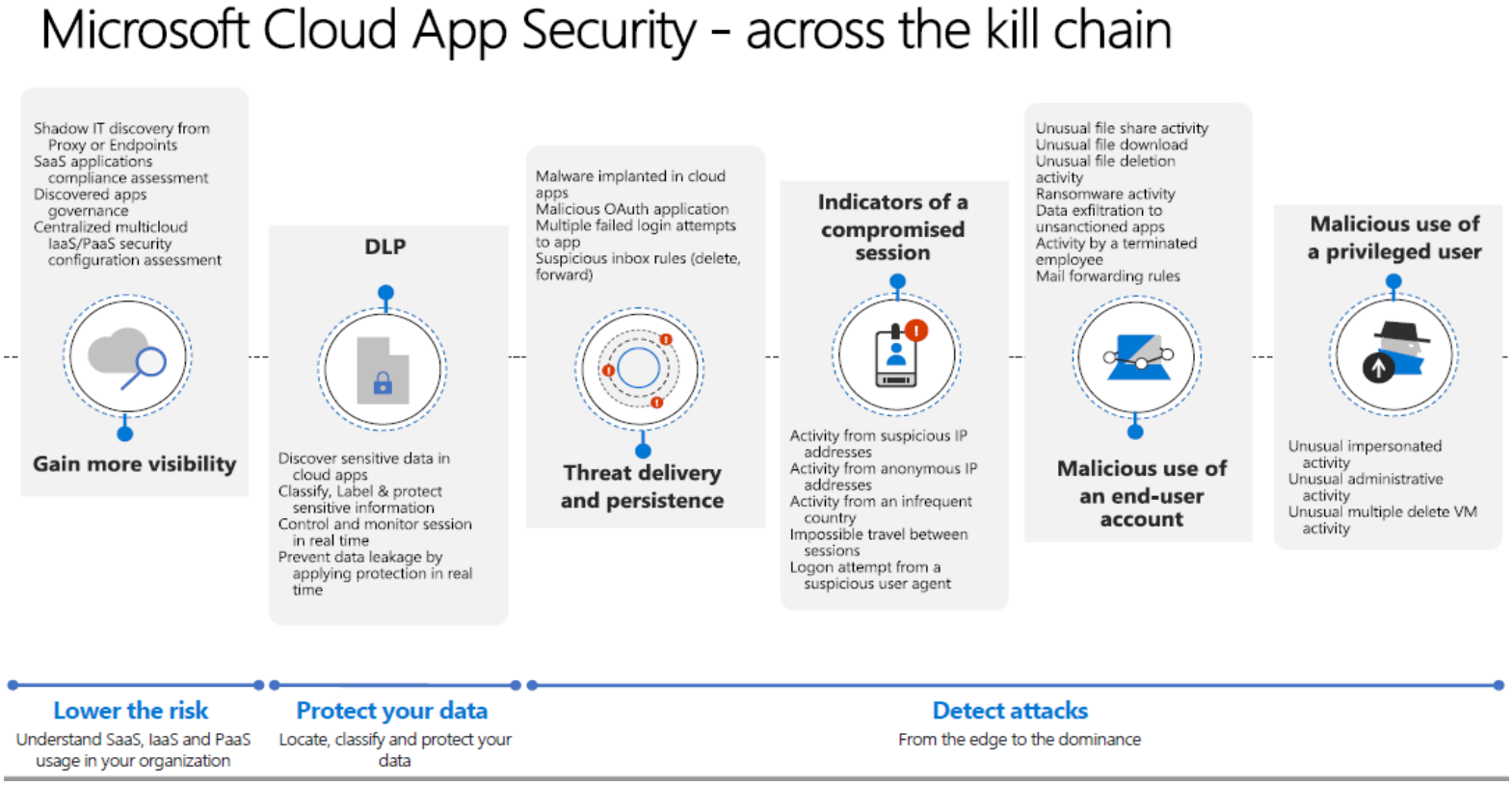


Figure 18 – 22: This document is referring to the **Tenable SC (Nessus) Vulnerability Scanning Software for Hays Global role in paragraph number 7.2** of this project, but the whole document is extracted from the Tenable SC allocation tool and ongoing workshop conducted by Tenable, its Design, Reviewing, function and Implementation at Hays for the Global Scanning by this sophisticated tool.

However, the full reports explained its (Tenable SC) design, function, and Implementation in Hays's ISMS environments. The full report is given below:

Reference *– Figure 18 illustrates more about the Tenable Design and plan, and workshop training Phase; however, for the GDPR all sensitive email Dada and Information is hidden.*

FW: Tenable/Hays Professional Services - Introduction

[redacted]

To [redacted]

Cc Hasan, AKM

Retention Policy EMEA & AMR - Default 7 year Delete (7 years) Expires 16/07/2029

Follow Up Information

You replied to this message on 18/07/2022 17:36.

Reply

From: [redacted]

Sent: 17 July 2022 09:39

To: [redacted]

Cc: [redacted]

Subject: Re: Tenable/Hays Professional Services - Introduction

thank you [redacted] for the introduction,

Dear [redacted],

Thank you for your trust in Tenable Professional Services.

I am the Professional Services Resource Manager and I'll be your Tenable contact to help you schedule and execute your QuickStart Optimise engagement.

This service is delivered in the following phases -

1. Phase 1: Design, Planning & Readiness
2. Phase 2: Implementation, Configuration & Enablement
3. Phase 3: Documentation

Please also see the respective service brief and the pre-call document attached for your reference.

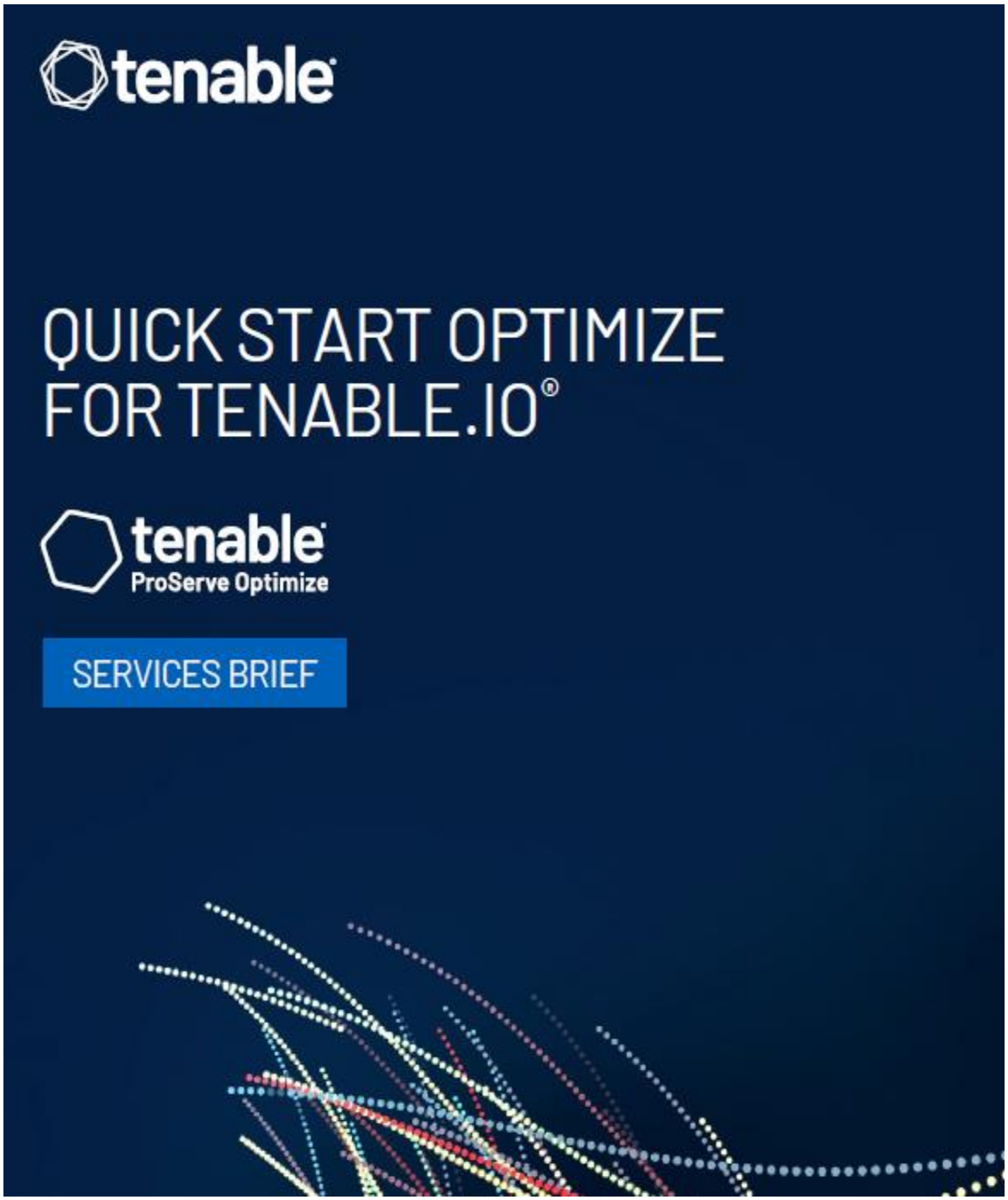
The design part of phase 1 will be delivered across two half day design workshops, followed by a design document that will be drafted by our consultant.

At the moment, we have availability **on August 8 and 9** to accommodate these sessions - please let me know what suits you best? I'll then send the respective invites over.

Once the design is approved and all prerequisites are ready, we will be in touch to agree on dates for phase 2, the implementation.

Looking forward to hearing from you.

Tenable SC Designing, Planning, Readiness, Implementation, Configuration and Enablement by conducting workshops through Tenable Specialist at Hays.


tenable
QUICK START OPTIMIZE FOR TENABLE.IO®
tenable
ProServe Optimize
SERVICES BRIEF

2. SERVICE OVERVIEW

Tenable.io® Quick Start Optimize services is a tailored service beginning with a Design and Planning Workshop to plan, design and guide towards adopting the Cyber Exposure Lifecycle and Risk-Based Vulnerability Management (RBVM) practices through the configuration and integration of a fully operational capability of Tenable.io.

This Quick Start service develops an organizational RBVM approach, leveraging Tenable's enterprise platforms and services to reduce overall Cyber Exposure risk.

This Quick Start Optimize Implementation is designed across three (3) key phases within the scope defined in this Brief:

Phase 1: Tenable Design and Planning, and Readiness

- **Design and Planning.** Experienced Tenable Consultants ("Consultant") will perform a one-day design and architecture workshop with Customer to agree on a solution design according to Tenable Best Practice and recommendations.
- **Readiness Exercise.** Experienced Tenable Consultants ("Consultant") will review and validate the solution design, prerequisites and specifications before Phase 2 - Implementation and Enablement commences.

Phase 2: Tenable.io Implementation, Configuration and Enablement

- **Install sensors and configure Tenable.io.** Nessus® sensors will be installed and configured based on requirements and will implement following Tenable's best practices for enterprise deployment captured during Phase 1 - Design and Planning.
- **Validate operational capabilities.** Tenable.io will be validated end to end for scanning and other operational capabilities.
- **Enablement.** Experienced Tenable Consultants ("Consultant") will provide a Tenable.io Enablement session guiding you through Tenable's best practices for Vulnerability Management.

Phase 3: Documentation and Project Coordination

- **Tenable Deliverable Documents.** Include Design and Architecture Workshop deliverable and Tenable.io documentation of your specific configuration of Tenable products post Installation provided for your future use.
- **Project Coordination.** Experienced Tenable Consultants ("Consultant") will provide ongoing Project Coordination and

2. SERVICE OVERVIEW

The Tenable.io® Web Application Scanning (WAS) Quick Start is a tailored service to streamline the identification and configuration of web application scanning.

This Quick Start Service is designed to provide five (5) outcomes within the scope defined in this Brief:

(a) **Plan and prepare the Customer**. Consultant will pre-plan, review and validate Tenable's approach and customer's prerequisites to ensure a smooth transition to Phase 2 activities.

(b) **Configure Tenable.io**. Tenable.io WAS will be initialized and configured by Consultant based on requirements captured during Phase 1 - Pre-Call.

(c) **Identified Scanning**. Consultant will scan up to ten (10) web applications (URLs) to provide a high-level assessment of the component vulnerabilities, HTTP security header, SSL/TLS and web application vulnerabilities.

(d) **Implement Tuning and Optimize Best Practices**. Consultant will implement and orient you to Tenable's best practices for future effective scanning

(e) **Provide Tenable Deliverable Document**. Document will provide a summary of your deployment requirements, deployed scanner resources and the web applications (URLs) identified for scanning.

However, this document is 19 pages of documents provided by Tenable to Hays's ISMS team but given a few of them to understand what the "**Tenable SC**" is helping Hays to control the security measure globally, these documents are given below:

Prerequisites

In order to receive the Quick Start services, the Customer must ensure before Tenable begins work that all of the following actions have been performed, are available or are accessible, as applicable:

(a) Tenable software covered by this Brief is downloaded and accessible to Engineer

(b) Customer has valid administrative usernames and passwords for software applicable to this Brief

(c) [redacted]

(d) Access to Tenable's Community and/or Support Portal

(e) All necessary hardware and appliances are mounted and in place

(f) Customer network topology diagram and information

(g) List of Customer hosts that can be actively scanned

(h) Administrative credentials for Customer hosts to be scanned

(i) Customer desired Tenable.io user list

(j) Customer SAML configuration file (if applicable)

(k) Connector information to cloud environment

Definitions

SAML

Security Assertion Markup Language – standard for exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider.

CIS

Center for Internet Security (CIS) – publishes the CIS Critical Security Controls (CSC) to help organizations better defend against known attacks by distilling key security concepts into actionable controls.

3. SCOPE

Tenable's Quick Start Optimize implementation is scoped across three (3) key phases organized by activities. Engineer will create and demonstrate in Tenable.io the following for up to 100,000 assets:

Phase 1: Activity 1 – Design and Architecture Workshop (Combination of remote and onsite delivery to be agreed)

(a) Tenable will perform a one-day Design and Architecture workshop with Customer to agree on a solution design

3. SCOPE

The Tenable.io WAS Quick Start will be delivered across four (4) phases, split into multiple categories:

Phase 1 - Pre-Call:

Requirements around WAS scanning and wider security objectives will be gathered during the pre-call, including an understanding of what environments are to be scanned (Development, QA, Pre-Production, Production). Prerequisites for scanning will be discussed to ensure that the customer environment is correctly prepared and configured for the Phase 2 activities.

Phase 2 - Initialization, Identification and Scanning Workshop:

The activities in Phase 2 may have been completed fully or partially in Proof of Value (PoV) deployment, but will be reviewed to ensure that operation is suitable for ongoing business activities.

(a) Access to the Tenable.io platform and WAS application will be confirmed.

(b) Consultant will ensure that the appropriate users have access to the Tenable.io WAS product for scanning and viewing of results. Role-Based Access Control (RBAC) will need to be defined to allow this access, and administrative credentials will be required for this configuration.

(c) If on-premises or remote scanner(s) are to be deployed, up to three (3) will be deployed and connected to Tenable.io. These scanners can be used for scanning internet-facing web applications or, if firewall rules are suitably configured, can be used to scan Development or Pre-Production environments. Tenable also offers the Tenable Core + WAS virtual appliance that can be deployed locally on-premises or within a cloud-based development environment to scan non-internet-facing web applications. The virtual appliance is available in .ova, .zip and .iso format from [redacted]r needs access to

Following the Initialization, Consultant will review the customer's security objectives gathered from the pre-call and recommend best practices. Consultant will explain the methodologies recommended to be used in Phase 3.

(a) The customer will identify up to ten (10) target web applications (URLs) to be within the scope of quick and detailed scanning.

(b) Methods for identifying further (possibly unidentified) web servers, services and applications using Tenable.io or Tenable.sc will be discussed.

(c) Consultant will utilize a preconfigured Python script to read an XLSX file to create a URL scan targeting the ten (10) URLs identified. The script requires Tenable.io access.

(d) Quick scans will be configured and deployed (or scheduled to be scanned) to provide a high-level assessment of the component vulnerabilities, HTTP security header, SSL/TLS and web application vulnerabilities.

(e) A review of the results from the quick scans will be done to:

(i) appraise the findings of the applications covered in "quick scan" only

(ii) review in detail the sitemap crawled as an input to the detailed scanning, tuning and optimization

Figure 23 and 24 - This document is referring to the **Implementing of Incident Response Management (IRM) by the ISMS team in paragraph number 7.3** of this project, but the whole document is extracted from the IRM process Playbook at Hays.

However, the full reports explained its (IRM) overview, scenario, and all other steps one by one if there were any incidents or data breaches (at Hays) then how employees and the ISMS team responded, as per the IRM Playbook. The full report is given below:

HAYS Working for your tomorrow

[redacted]

IRM PLAN and overview

Hays IRM plan/ Incident Response Management Plan (Updated version for 2022 [redacted] Guidelines and Directions for the Overall IRM Desktop Exercise.

When an incident or potential incident take place at Hays, whether it is related to data breaches or security-related issue, then it triggers the IRM process, and then the relevant teams and Personnel start their process, as per the IRM Playbook.

All procedures and steps are in place at Hays for the IRM, but these IRM documents are extra precautions for Hays Cyber and ISMS team to oversee the process, as a whole in a simpler and faster way.

[redacted] and in order to ared and well

For the next Phase follow document 01 - a) >>

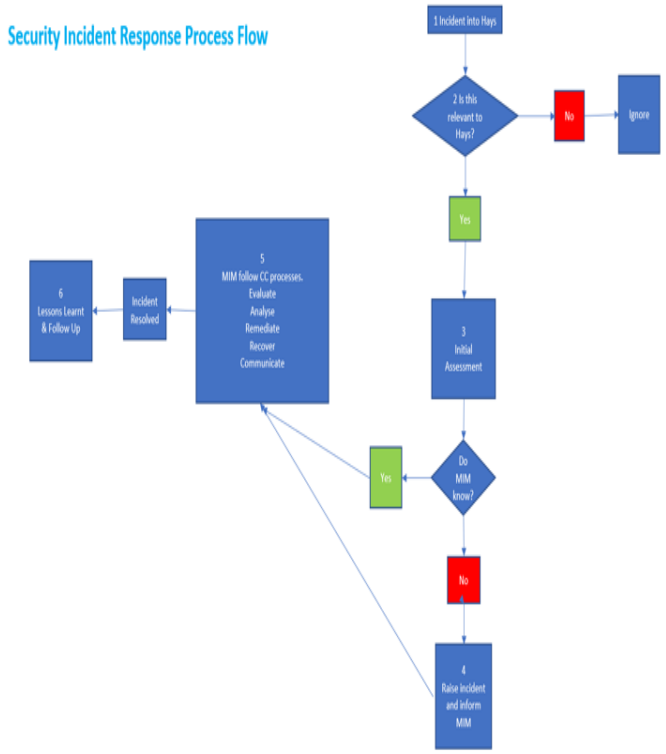
HAYS Working for your tomorrow

[redacted]

Call Tree and Flow Chart Elucidation

Hays [redacted] in of Communication and maintain the Cl[redacted]anagement (IRM) process. This docu[redacted]Cyber Security Manager and from Information Security Officer.

However, for the Incident Management Process, Personnel must follow the flow chart at Hays and CC in order to tackle the circumstances.



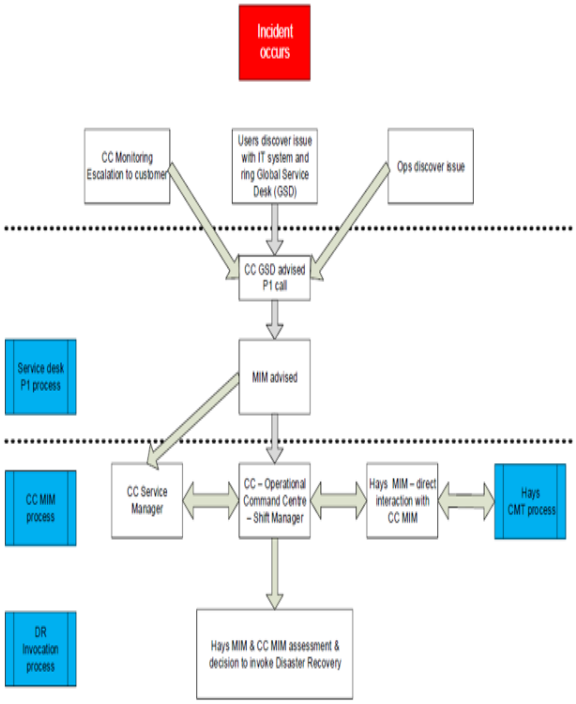
HAYS Working for your tomorrow

Find the flow chart for the CC below:

HAYS Recruiting experts worldwide

Computacenter

6.2 [redacted]



For the next Phase follow document 02 >>

SCENARIO:
A Hays user has reported to the Service Desk that he has tried to open a document on a shared drive. The document has not opened correctly and the screen is displaying a message.

What happens now?

[redacted]

HAYS Working for your tomorrow

[redacted]

INCIDENT RECOVERY

[redacted] should be gathered and piled full disaster recovery reports, including its finding, observations, and recommendations for making the Hays BAU process functional.

For the next Phase follow document 04 >>

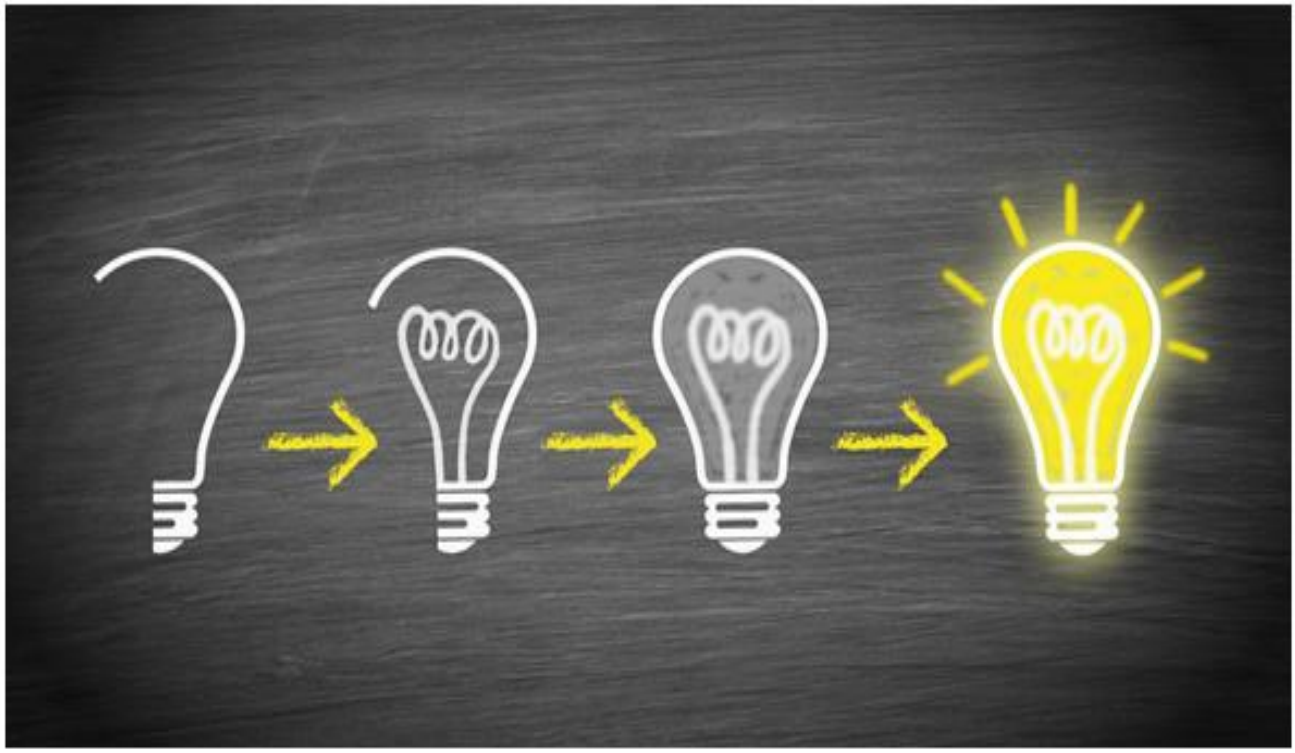
HAYS Working for your tomorrow

[redacted]

LESSONS LEARNED

[redacted] the overall Lessons Learned from the incidents, including what type of Gap analysis should be Implemented for Hays Cyber and IT Security, and must carry out for its Cyber defense.

In this report, all elements will be highlighted.



For the next Phase follow document 05 >>

HAYS Working for your tomorrow

Doc 05

BACK TO BUSINESS

This Phase is giving the indication that the IRM process has been completed and [redacted] rectified and neutralised, and the whole IRM process [redacted]

Moreover, this Phase will add additional reports, which will be called Director's observations, which means, the IT Services Product Director and his security Team (Cyber and ISMS) will provide another layer for the Incident Response Management (IRM), wherein will provide additional views based on Doc 01 - 04, as per new and current laws and Hays IRM requirements.

"The IRM Phase Conclude Here"

Figure 25 – This document is referring to the **Risk Assessment for the Project Management and Risk Analysis in paragraph number 8** of this project, but the whole document is extracted from Google to evaluate why this Project risk is Extreme category.

Likelyhood	Consequences				
	Insignificant *Risk is easily mitigated by normal day to day process*	**Minor** *Delays up to 10% of Schedule Additional cost up to 10% of Budget*	**Moderate** *Delays up to 30% of Schedule Additional cost up to 30% of Budget*	**Major** *Delays up to 50% of Schedule Additional cost up to 50% of Budget*	**Catastrophic** *Project abandoned*
Certain *>90% chance*	High	High	Extreme	Extreme	Extreme
Likely *50% - 90% chance*	Moderate	High	High	Extreme	Extreme
Moderate *10% - 50% chance*	Low	Moderate	High	Extreme	Extreme
Unlikely *3% - 10% chance*	Low	Low	Moderate	High	Extreme
Rare *<3% chance*	Low	Low	Moderate	High	High

Appendices – ***All other factors*** have been captured in **Appendices** in this Research Project.

<u>Figure 26</u> - This document is referring to ***External Audit Trail at Hays by PWC*** **in paragraph number 14.1** of this project, but the whole document is extracted from PWC's Assessments and Audit reports to Hays.

The full report is given below:

4. Internal Controls

IT audit scope & approach

Our IT audit testing [redacted] the processing and recording of financial data operati[redacted]any, and Australia.

While we plan for our [redacted]nsistent with previous periods), we are required by auditi[redacted] and evaluated the Group's control environment, includin[redacted]

We have completed [redacted] to IT General Controls (ITGCs) supporting the Hays [redacted] Our ITGCs audit focused on the following domains:

- **User Access Management** – [redacted]cation and monitoring.
- **Change Management** – mod[redacted]ng programs and data.
- **Computer Operations** – bac[redacted]n jobs, and disaster recovery.
- **Program Development** – de[redacted] more significant than individual changes.

[redacted]ermany as a result of this work. Set out in this [redacted](including on those systems relevant at a Group level).

Applications assessed from the Group

System	System used by	Audit procedures undertaken
PeopleSoft Financial Reporting	UK and Ireland	Walkthrough procedures (Inquiry and Inspection)
HFM	Group and operational companies	
LOIS LLA	Group	
ONEtouch	PeopleSoft Financial Reporting	Process and control understanding (Inquiry)
3SS (3 Story Software)	Operating companies	

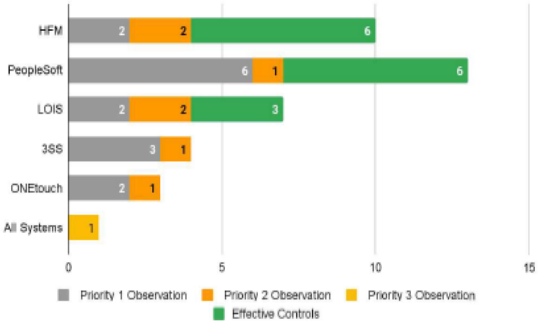
Improvements, observations and global outlook

We hav[redacted]e control environment with respect to monitoring of third party service [redacted]inimum controls framework, and robustness of documentation to demons[redacted]ols. We have identified 23 IT control observations across all the systems[redacted]es* relevant for financial reporting of which 15 were considered a Priority[redacted]ing. Our priority 1 observations have been group together and detailed[redacted]

We hav[redacted]homogeneity of IT General Controls and extensive use of different third pa[redacted]y.

[redacted]

Observations and effective controls



1 A significant control weakness to be addressed as soon as possible.

2 A control weakness to be addressed within next 12 months.

3 Recommendations that are best practice in nature to be addressed within 12 months.

Effective controls

Key observations on IT General controls

Privileged access monitoring: [redacted]urrently operate formal transactional level monitoring of the activities execute[redacted]counts across in scope finance systems. This increases the risk that privileged [redacted] circumvent system enforced authorisation checks, bypass segregation of duties[redacted]d changes to data and system configuration which go undetected.

Privileged user access review: [redacted]rtification over privileged accounts for all finance systems. Th[redacted]g inappropriate access to systems which increases the risk of i[redacted]ivity.

Change management: The finance systems are not able to produce system based change logging reports that capture a complete list of all changes to the code and configuration within the application. This increases the risk that script based changes are released directly into the production environment (due to lack of Segregation of Duties) bypassing the change management process and hence going undetected. Sufficient alternative controls should be implemented to reduce the identified risk.

Assurance activities over Third Parties: [redacted]s of IT service management to a number of third part[redacted]ols that operate at the IT infrastructure layer (i.e. [redacted] formal independent third party service organisation c[redacted] SOC 1 Type 2 report) over controls operated by the th[redacted]ne third party provider exists this has not been exercised.

PwC • 11

However, this document is 65 pages but given a few of them (based on security prospects) to understand what is "PWC External Audit trail" is and how the ISMS team Implement their (PWC) recommendation Change Management based on this document. Black masks cover data and Information due to GDPR and Hays's Commercial Confidentiality Policy. These documents are given below:

4. Internal Controls

Data enabled IT audit procedures in response to Covid-19

Given the continued [redacted] onment, to address the increased risk of potential unautho[redacted] financial systems, we performed data enabled audit proce[redacted] going effectiveness of management's user access manager[redacted] used on assessing the timely removal of access rights for t[redacted]

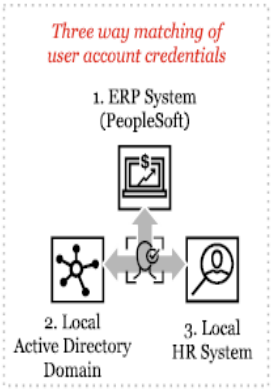
Testing approach and observations posing a risk to financial reporting

We performed a series of reconciliations between the three datasets to identify any accounts on PeopleSoft ERP system which pose a risk to financial reporting.

[redacted] sts was performed for the review period,

- [redacted] list of active users from PeopleSoft who are not
- [redacted] the list of users that logged into Active Directory [redacted] ination date based on the HR list and Last sign on [redacted] ft ERP system with focus on the Finance Module.

Three way matching of user account credentials



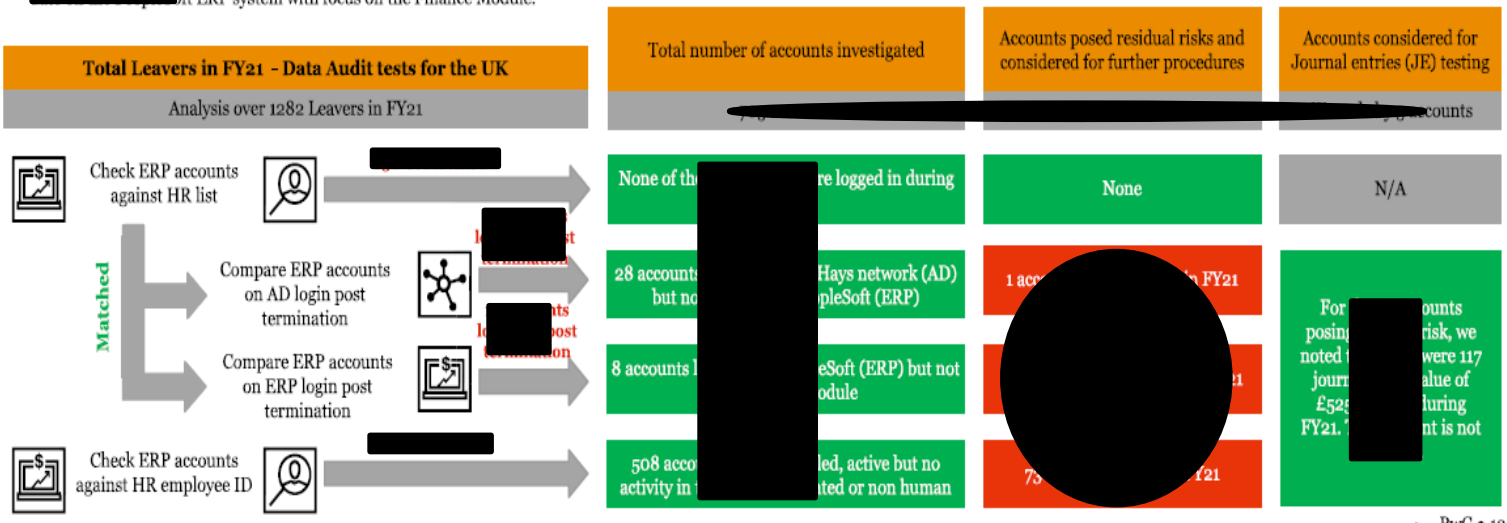
Observations for informational analysis

The followi[redacted] rmed for informational purposes and hence was perfor[redacted] the interim period 01/07/2020 to 31/03/2021;

- [redacted] active AD accounts that are not captured on HR
- [redacted] HR records that do not have a matching

Through this data exercise, we identified about 400 accounts that are active on PeopleSoft as of [redacted] ut have not been accessed in the FY21 reporting period, of which [redacted] not been accessed since set up. Management can consider wh[redacted] unts can be disabled to reduce the number of accounts that n[redacted] ied on a periodic basis.

Through our inv[redacted] oted that management has improved the robustness of ev[redacted] for most of the Leavers controls to demonstrate the operation of [redacted] ired for audit purposes.



External Audit by PWC

4. Internal Controls

IT audit scope & approach

Our IT audit testi[redacted]ems responsible for the processing and recording of financial data oper[redacted]st markets - UK, Germany, Australia, France. These markets represent[redacted]d across the Group.

Given the decentra[redacted]T landscape, each local market IT audit team updated their understandi[redacted]sses operating. Where appropriate, we assessed the corresponding des[redacted]neral Controls (ITGCs) across the IT domains. Where the local audit tea[redacted]e system, ITGCs have been assessed across the year:

- **User Access Management** – [redacted]hanges and revocation
- **Change Management** – modi[redacted]enance of IT application's underlying programs and system configurat
- **Computer Operations** – back[redacted]ch jobs and disaster recovery
- **Program Development** – lar[redacted] and programmes

Based on the outcome of our updated understanding of both the local IT landscape and control environment our financial audit teams were able to plan the most effective and efficient audit strategy for their territory. This is summarised in the table below:

Market	IT System	Reliance on system	Method of assessing the risks arising from the IT systems and related IT dependencies
Group Finance	Consolidation (HFM) & LOIS	No	[redacted]ures performed as part of the year end close [redacted]ot been tested.
United Kingdom	PeopleSoft	No	[redacted]ures enhanced by a data enabled evaluation [redacted]The migration in Ireland has been [redacted]ntive audit procedures.
Germany	SAP	Partial	[redacted]ures enhanced by a data enabled evaluation [redacted]Limited testing of ITGCs are performed to [redacted]misstatement.
Australia	Great Plains	No	[redacted]ures performed as part of the year end close [redacted]ot been tested.
France	Microsoft Dynamics NAV	No	[redacted]ures enhanced by a data enabled evaluation [redacted]Limited testing of ITGCs are performed to [redacted]misstatement.

Note 1: IT dependencies are tested as part of the planned substantive audit procedures.

Our conclusion

- [redacted]we have not placed reliance on the finance systems a[redacted]up. In [redacted]e continue to face challenge in ensuring that users ca[redacted]he [redacted]or privileged account monitoring controls and the in[redacted] of [redacted]ties.
- [redacted]y unauthorised postings made to the finance systems by leavers who had [redacted]after their leaving date.
- [redacted]gement continue to focus on th[redacted]ation of a [redacted]ral Control (ITGC) framework a[redacted]g upon the [redacted]ntrols project.
- [redacted]risk assessment indicat[redacted]six risks remain with a higher net [redacted](i.e. after mitigations). [redacted]s is needed on ensuring effective [redacted]place to mitigate the sp[redacted]yber risks.

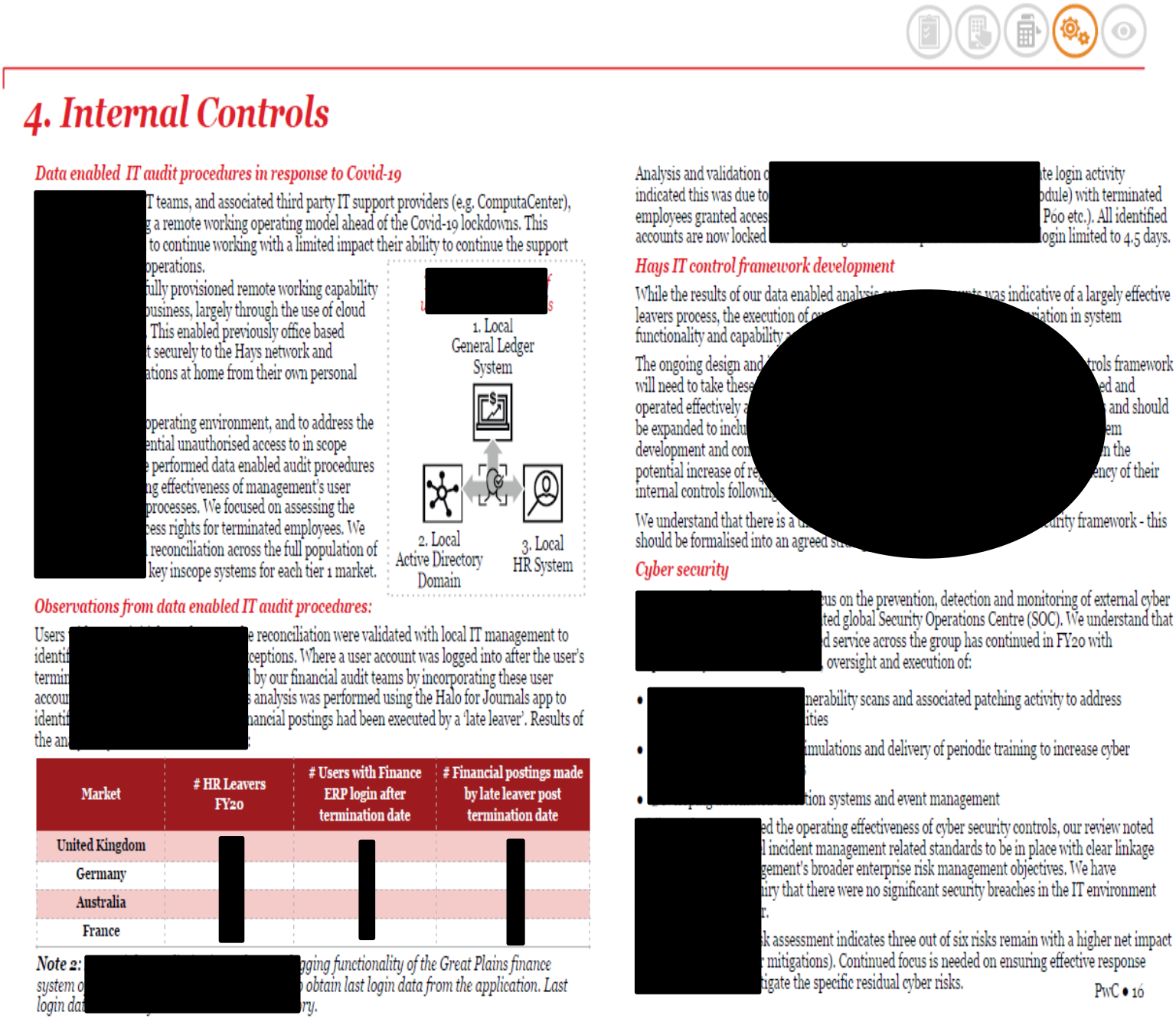
Areas of focus for IT controls

While the Hays IT function has a defined set of policies and procedures in place, we recommend particular attention is focused on the following elements of the internal control that continue to preclude us from placing further reliance on IT systems, primarily:

Change Management: Local f[redacted]vent inability to produce system based c[redacted]listing of all changes to the pr[redacted]. This includes script based cha[redacted]environment which could potentially bypass the [redacted] process. UK AU FR

Privileged Access Monitoring: Ma[redacted]y operate formal transactional level mo[redacted]ged user accounts across in sco[redacted] privileged users could poten[redacted]on checks, bypass segregation of du[redacted]s to data and system configuration. UK AU FR

Assurance of activities performed by third parties: Hays have outsourced responsibi[redacted]ement to a number of t[redacted]ols that ope[redacted]do not obtain any formal in[redacted]rance reports (e.g ISAE 3402 / S[redacted]hird party on its behalf. While the right to audit the third party provider exists this has not been exercised. UK AU DE FR



4. Internal Controls

Data enabled IT audit procedures in response to Covid-19

[redacted] T teams, and associated third party IT support providers (e.g. ComputaCenter), g a remote working operating model ahead of the Covid-19 lockdowns. This to continue working with a limited impact their ability to continue the support operations.
fully provisioned remote working capability business, largely through the use of cloud This enabled previously office based t securely to the Hays network and ations at home from their own personal

operating environment, and to address the ential unauthorised access to in scope performed data enabled audit procedures ng effectiveness of management's user processes. We focused on assessing the cess rights for terminated employees. We reconciliation across the full population of key inscope systems for each tier 1 market.

[redacted]
1. Local General Ledger System
2. Local Active Directory Domain
3. Local HR System

Observations from data enabled IT audit procedures:

Users [redacted] e reconciliation were validated with local IT management to identif ceptions. Where a user account was logged into after the user's termin by our financial audit teams by incorporating these user accou analysis was performed using the Halo for Journals app to identif ancial postings had been executed by a 'late leaver'. Results of the an

Market	# HR Leavers FY20	# Users with Finance ERP login after termination date	# Financial postings made by late leaver post termination date
United Kingdom	[redacted]	[redacted]	[redacted]
Germany			
Australia			
France			

Note 2: [redacted] *gging functionality of the Great Plains finance system o obtain last login data from the application. Last login da ry.*

Analysis and validation o [redacted] te login activity indicated this was due to odule) with terminated employees granted acces P60 etc.). All identified accounts are now locked ogin limited to 4.5 days.

Hays IT control framework development

While the results of our data enabled analysis was indicative of a largely effective leavers process, the execution of ou iation in system functionality and capability

The ongoing design and trols framework will need to take these ed and operated effectively a and should be expanded to inclu em development and con n the potential increase of re ency of their internal controls following

We understand that there is a u urity framework - this should be formalised into an agreed st

Cyber security

[redacted] us on the prevention, detection and monitoring of external cyber ted global Security Operations Centre (SOC). We understand that d service across the group has continued in FY20 with oversight and execution of:

- [redacted] nerability scans and associated patching activity to address ities
- imulations and delivery of periodic training to increase cyber
- tion systems and event management

[redacted] ed the operating effectiveness of cyber security controls, our review noted l incident management related standards to be in place with clear linkage gement's broader enterprise risk management objectives. We have iry that there were no significant security breaches in the IT environment r.

k assessment indicates three out of six risks remain with a higher net impact mitigations). Continued focus is needed on ensuring effective response igate the specific residual cyber risks.

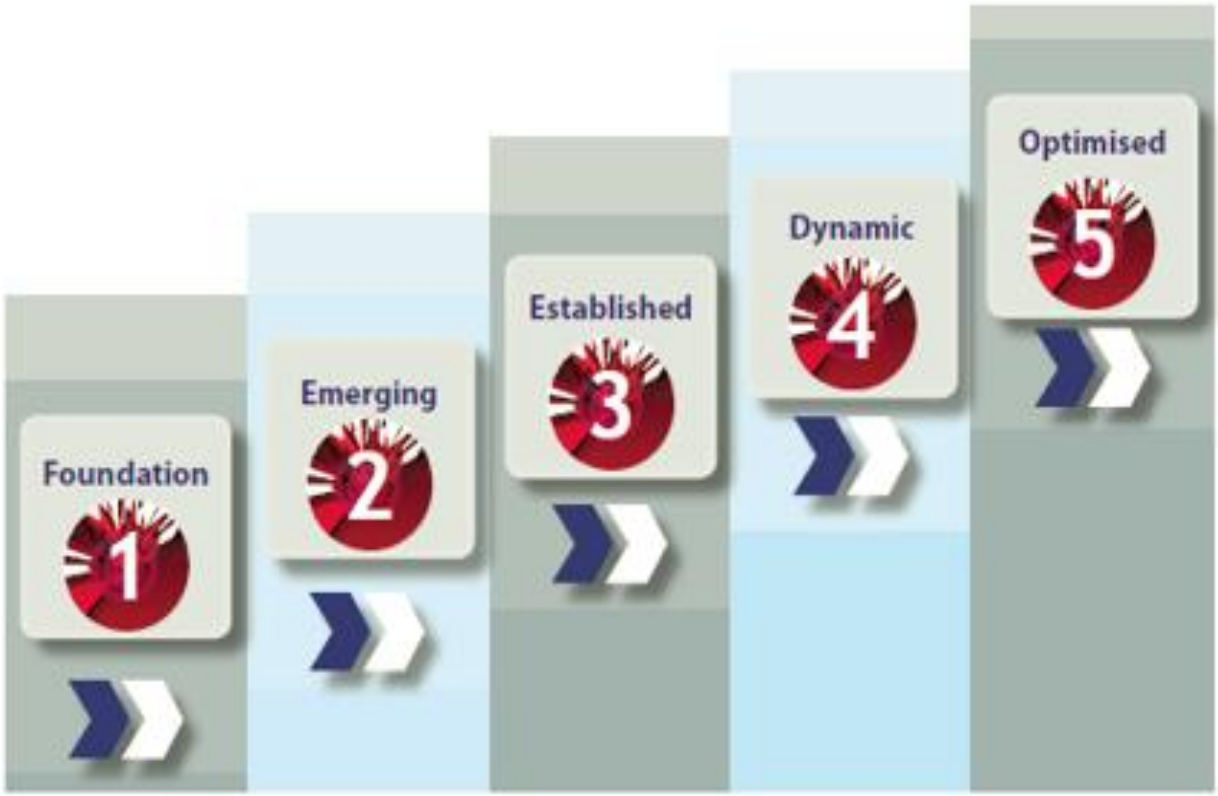
PwC • 16

<u>Figure 27</u> - This document is referring to ***External Audit Trail at Hays by KPMG*** **in paragraph number 14.1** of this project, but the whole document is extracted from KPMG's Assessments and Audit reports to Hays.

The full report is 29 pages, therefore, only provides the main diagram for it to understand its reader hat how KPMG conducted an external Audit at Hays for ***Pen Testing*** Advisory Review. Alongside this, I am adding the current external Audit is ongoing at Hays by KPMG in Jul 2022; therefore, I am adding its background and scope (draft version from KPMG) to understand how they conduct external Audits at Hays. These are given below:

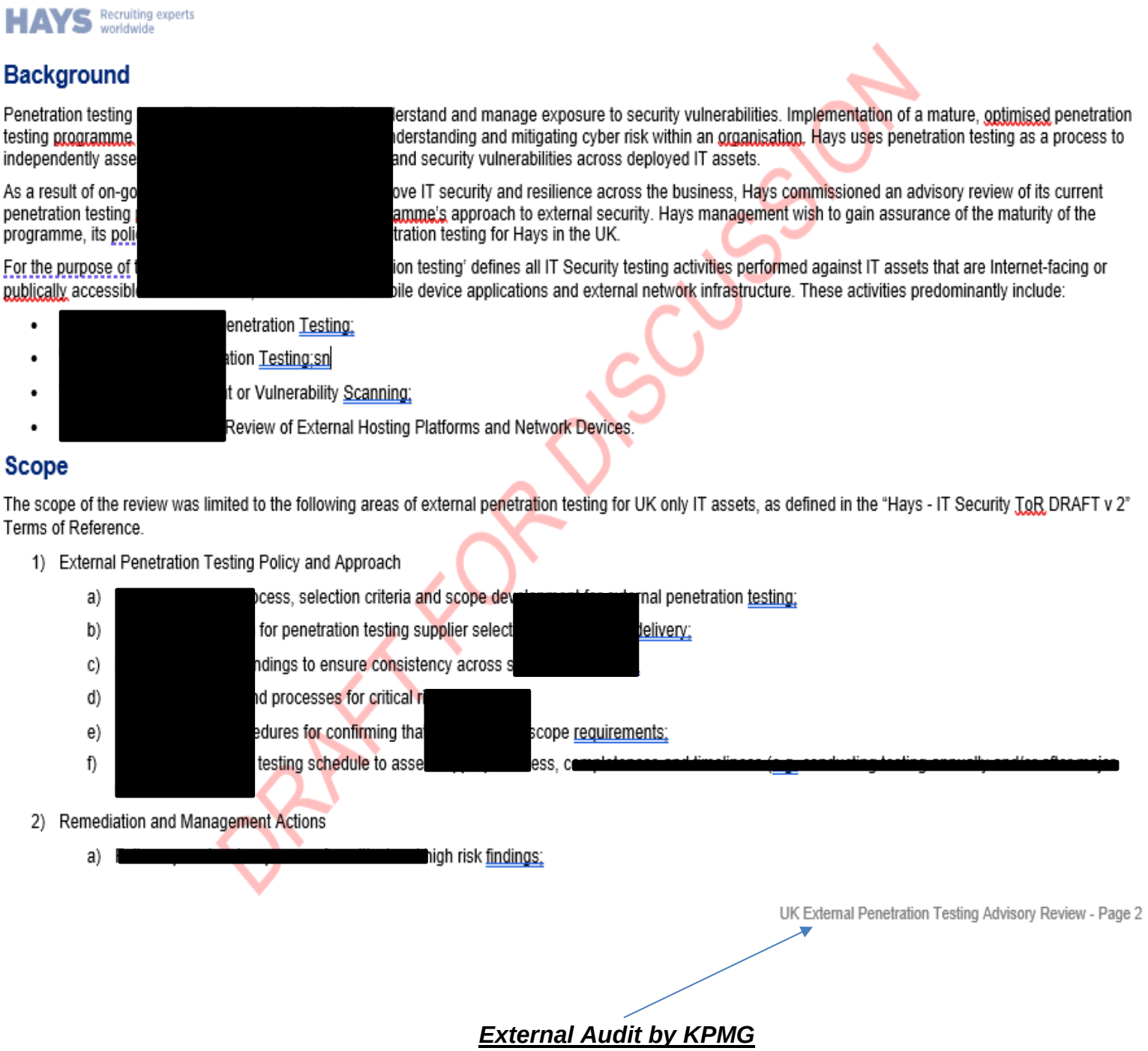
HAYS Recruiting experts worldwide

[redacted] CREST Penetration Testing Programme Maturity Model



[redacted]

Figure 1 - CREST Penetration Testing Programme Matur[redacted]ed.org/)



HAYS Recruiting experts worldwide

Background

Penetration testing [redacted] erstand and manage exposure to security vulnerabilities. Implementation of a mature, optimised penetration testing programme [redacted] derstanding and mitigating cyber risk within an organisation. Hays uses penetration testing as a process to independently asse[redacted] and security vulnerabilities across deployed IT assets.

As a result of on-go[redacted] ove IT security and resilience across the business, Hays commissioned an advisory review of its current penetration testing [redacted] amme's approach to external security. Hays management wish to gain assurance of the maturity of the programme, its poli[redacted] tration testing for Hays in the UK.

For the purpose of t[redacted] ion testing' defines all IT Security testing activities performed against IT assets that are Internet-facing or publically accessibl[redacted] ile device applications and external network infrastructure. These activities predominantly include:

- [redacted] enetration Testing;
- [redacted] ation Testing;sn
- [redacted] t or Vulnerability Scanning;
- [redacted] Review of External Hosting Platforms and Network Devices.

Scope

The scope of the review was limited to the following areas of external penetration testing for UK only IT assets, as defined in the "Hays - IT Security ToR DRAFT v 2" Terms of Reference.

1) External Penetration Testing Policy and Approach
   a) [redacted] cess, selection criteria and scope dev[redacted] nal penetration testing;
   b) [redacted] for penetration testing supplier select[redacted] delivery;
   c) [redacted] ndings to ensure consistency across s[redacted]
   d) [redacted] d processes for critical r[redacted]
   e) [redacted] edures for confirming tha[redacted] scope requirements;
   f) [redacted] testing schedule to asse[redacted] ess, c[redacted]
2) Remediation and Management Actions
   a) [redacted] high risk findings;

External Audit by KPMG

Figure 28 and 29 - This document is referring to **Internal VA** by Q&O IT Group **in paragraph number 14.2** of this project, but the whole document is extracted from A&O IT Group's Internal Vulnerability Scanning reports to Hays.

The full report is very large, therefore, only provides a few of them to understand its reader hat how A&O conducted an Internal VA at Hays. These are given below:

A	B	C	D	E	F	G	H	I	J
Scan Date	Scanner	IP Address	Tag	OS	Discovered Name	System Owner	Description (Asset register)	Hays Rating	Vulnerability Category
May-22	qualys	[redacted]	Manchester	EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux 3.x / IBM / FortiSOAR	hrmnxpd4075	CC	RFW2426 - Ubuntu[redacted]	Low	Patch Maintenance and Configuration
May-22	qualys		Manchester	Windows 2012 R2/8.1	hrmvmpd3406.er	CC	[redacted] Web	Low	Patch Maintenance and Configuration
May-22	qualys		Manchester	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP / Integrated	INFO Not Found	CC	INFO Not Found	Low	Data Transport
May-22	qualys		Romford	Microsoft Windows 10	hrrvmpd4832.em	CC	[redacted] SO VMs	Low	Patch Maintenance and Configuration
May-22	qualys		Manchester	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP / Integrated	INFO Not Found	CC	INFO Not Found	Low	Services
May-22	nessus		Manchester	AIX 7.1	hrmmgam06	CC	A[redacted] Server	Low	General
May-22	nessus		Manchester	AIX	hrmmgam06-pro	CC	A[redacted] - NIM Server	Low	General

K	L	M	N
Vulnerability Title	**Protocol / Port**	**Vulnerability Description**	**Scanner Rating**
.user.ini File Information Disclosure Vulnerability	TCP / [redacted]		Medium
Account Brute Force Possible Through IIS NTLM Authentication Scheme	TCP / [redacted]		Low
Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	TCP / [redacted]		Medium
Account Brute Force Possible Through IIS NTLM Authentication Scheme	TCP / [redacted]		Low
Deprecated SSH Cryptographic Settings	TCP / [redacted]		Medium

O	P	Q	R	S
CVSSv2	**CVE**	**Diagnosis**	**Recommended Solution**	**Data Collected**
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	N/A	Since PHP 5.3.0, PHP includes support for ="https://secure.php.net/manual/en/configuration.file.per-user.php" TARGET="_blank">.user.ini configuration files	Customers as advised to protect their .user.ini files from unauthenticated access by implementing security solutions	Sensitive .user.ini file detected on port: 443. GET /.user.ini HTTP/1.0 Host: [redacted]
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	CVE-2[redacted]9	NTLM authentication is enabled on the Micros	currently there are no vendor supplied patches available for this issue. Workaround 1) Disable NTLM	GET / HTTP/1.0 Host: [redacted] Authorization: NTLM TlRMTVNTUAABAAAAA7IAAAAAAAAAAAAAAAA
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	CVE-2[redacted]3	Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support	Disable and stop using DES, 3DES, IDEA or RC2 ciphers. More information can be found at: "https://sweet32.info/"	CIPHERKEY-EXCHANGEAUTHENTICATIONMACENCRYPTION(KEY-STRENGTH)GRADE GET / HTTP/1.0
5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	CVE-2[redacted]9	NTLM authentication is enabled on the Micros	currently there are no vendor supplied patches available for this issue. Workaround 1) Disable NTLM	Host: [redacted] Authorization: NTLM TlRMTVNTUAABAAAAA7IAAAAAAAAAAAAAAAA
6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)	N/A	The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another. The target is using deprecated SSH	Avoid using deprecated cryptographic settings. Use best practices when configuring SSH	TypeName key exchangediffie-hellman-group1-sha1 ciphe[redacted] cipherblowfish-cbc
7.5	CVE-[redacted]19		Upgrade to Apache version 2.4.53 or later.	
7.5	CVE-[redacted]19		Upgrade to Apache version 2.4.53 or later.	

Figure 30 and 31 - This document is referring to **External VA** by NCC Group **in paragraph number 14.2** of this project, but the whole document is extracted from NCC Group's External Vulnerability Scanning reports to Hays.

The full report is very large, therefore, only provides a few of them to understand its reader hat how A&O conducted an Internal VA at Hays. These are given below:

nccgroup

Managed Security Monitoring Service
Technical Report for Hays Specialist Recruitment

HAYS Recruiting experts worldwide

External VA
10 June 2022

Vulnerability Assessment - Summary

Vulnerability Monitoring Summary

The NCC Group managed security monitoring service regularly performs vulnerability scans against your external infrastructure. Below are the details of your most recent **2** scan(s) that have been conducted against your infrastructure.

The table below gives a high level overview outlining the status of your infrastructure for the reporting period.

External VA & Daily Delta

Scan Start Date	Vulnerabilities Discovered	High Vulnerabilities	Medium Vulnerabilities	Low Vulnerabilities	Ignored Vulnerabilities
10 June 2022	[redacted]				0
04 March 2022					0

A	B	C	D	E	F	G
Company Name	Customer Incident ID	IPv4	Host Label	Port Number	Service Name	CVSSv2
Hays Specialist Recruitment	[redacted]15	[redacted]	Torino	[redacted]/tcp	HTTPS	7.1
Hays Specialist Recruitment	[redacted]23	[redacted]	Torino	[redacted]/tcp	HTTPS	7.1
Hays Specialist Recruitment	[redacted]37	[redacted]	Amsterdam	[redacted]/tcp	HTTPS	7.1
Hays Specialist Recruitment	[redacted]31	[redacted]	Amsterdam	[redacted]/tcp	HTTPS	7.1
Hays Specialist Recruitment	[redacted]77	[redacted]	[redacted]	[redacted]/tcp	HTTPS	7.1
Hays Specialist Recruitment	[redacted]82	[redacted]	[redacted]	[redacted]/tcp	HTTPS	7.1

CVSS Vector	Severity	Vulnerability Title
(AV:N/AC:H/Au:N/C:C/I:C/A:N)	High	[redacted] Certificate Subject CN Does Not Match the Entity Name
(AV:N/AC:H/Au:N/C:C/I:C/A:N)	High	Certificate Subject CN Does Not Match the Entity Name
(AV:N/AC:H/Au:N/C:C/I:C/A:N)	High	Certificate Subject CN Does Not Match the Entity Name
(AV:N/AC:H/Au:N/C:C/I:C/A:N)	High	Certificate Subject CN Does Not Match the Entity Name
(AV:N/AC:H/Au:N/C:C/I:C/A:N)	High	Certificate Subject CN Does Not Match the Entity Name
(AV:N/AC:H/Au:N/C:C/I:C/A:N)	High	Certificate Subject CN Does Not Match the Entity Name

IP Address	Label	rDNS Names	Port Number	Protocol	Service Name	Service Prduct
[redacted]			[redacted]	tcp	HTTP	
				tcp	HTTPS	Microsoft-HTTPAPI
				tcp	HTTP	
				tcp	unknown	
				tcp	unknown	
				tcp	HTTPS	HTTP
				udp	SNMP	
				tcp	bgmp	
			64	tcp	HTTP	Firewall-1
				tcp	bgmp	
			64	tcp	HTTP	Firewall-1
				tcp	bgmp	
			64	tcp	HTTP	Firewall-1
	NOIDA			udp	SNMP	
	NOIDA			udp	SNMP	
	NOIDA			udp	SNMP	
		web01haysspain.northeurope.cloudapp.azure.com		tcp	HTTP	Microsoft-HTTPAPI
		web01haysspain.northeurope.cloudapp.azure.com		tcp	HTTPS	Microsoft-HTTPAPI
	NOIDA			tcp	BGP	
				tcp	SSH	
				tcp	BGP	

Severity	Count of Solution Group
High	[redacted]
SSL enabled Services are not configured securely	
Systems were identified to be running out of date Pulse Connect Secure which may be vulnerable to exploitation and requires updating.	
SSH was identified to be out of date and requires patching	
Services require reconfiguration to follow best security practice	
The server supports authentication methods in which credentials are sent in plaintext over unencrypted channels.	
Medium	
SSL enabled Services are not configured securely	
SSH was identified to be out of date and requires patching	
Services require reconfiguration to follow best security practice	
Linux Packages were identified to be out of date and requires patching	
Low	
SSL enabled Services are not configured securely	
SSH was identified to be out of date and requires patching	
Services require reconfiguration to follow best security practice	
Additional information collected during the course of the test	
Web Application configuration requires updating to maintain application security	
Grand Total	

Figures 32, 33, and 34: - This document is referring to **Penetration Testing by the NCC** Group **in paragraph number 14.3** of this project, but the whole document is extracted from the NCC Group's Penetration Testing reports to Hays.

The full report is 35 pages, and the management report is 5 pages, therefore, only provides the main management chart from it, and a few from the main reports to understand its reader hat how the NCC Group conducted Penetration Testing at Hays. These are given below:

The Management Report Synopsis is given below:

ICO Programme - Pen Test Management Response

A Pen test was carried out by NCC Group at Reading office post the proof-of-concept conversions of both Reading and Croydon offices. The results of these findings have been delivered by NCC Group to Hays and stored in full in SharePoint here.

Below is a table of the High and Medium issues found during the exercise, some commentary, suggestions for closing the issue, the Owner of the issue and the management response:

Finding	Commentary	Management Response	Owner
1. HIGH – Paxton MSSQL	This [redacted] and prop [redacted] ired to rem [redacted] s of loca [redacted] te the risk as per [redacted]	Acknowledged, ICO [redacted] ly. This risk appl [redacted] y systems and does not res [redacted] The risk will i [redacted] Point 4	[redacted]
2. High – default net2 credentials	This [redacted] and prop [redacted] ired to rem [redacted] s of loca [redacted] te the risk as per [redacted]	Acknowledged, ICO [redacted] ly. This risk appl [redacted] y systems and does not res [redacted] The risk will i [redacted] Point 4	[redacted]
3. High – Passwords on physical media	Shar [redacted] own limit [redacted] lution for Paxt [redacted]	Acknowledged, but I [redacted] The need for [redacted] moved once the device is [redacted] sign.	[redacted]
4. High – Door entry exposed	Diffi [redacted] vice needs to b [redacted] network to allo [redacted] roperties and [redacted] d iden [redacted] to work.	Acknowledged, ICO [redacted] ly. This risk applies to al [redacted] s and does not result from work for [redacted]	[redacted]

1 Executive Summary

This report presents the findings of the zero trust network security assessment conducted on behalf of Hays Specialist Recruitment (Hays). The assessment was conducted between 14/03/2022 and 18/03/2022.

The system being assessed was part of Hay's move away from the traditional trusted office design to a zero-trust Internet connected design. This model has been initially piloted in two offices although the security assessment was carried out in a single location, the Reading office.

Overview

The security posture of the systems within scope was found to be appropriate to the assets which required protection. However, it was also noticeable that the majority of the risk to the network was presented by a small number of the observed devices. A number of high risk issues were identified which should be addressed if the organisation's security model is to maintain an appropriate defence in depth basis. The findings also illustrate the importance of ensuring that an otherwise robust security model cannot be undermined by isolated weaknesses.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
External Infrastructure	0	0	0	0	**0**
Internal Infrastructure	0	[redacted]			
Total	**0**				

Assessment Summary

The security assessment w components, testing from an external perspective and testing fro The external testing showed that only a minimal set of services w offices. This limited the opportunity for attack and no security . The internal assessment was further split into an initial p llowed by later white box tests which made use of informa initial black box testing identified a number of networks, some ed as intended. This was evidence of poor IT practices and the c d give an attacker access to services which should not be expos

Additionally, a number of w d insecurely and exposed encrypted credentials of a domain us a position on the network which allowed them to intercept t orkstation, could capture the encrypted credentials. Dur ain user credentials was obtained exploiting this weakness. H n which these workstations were used within the office, it sh ttacker with more time would recover more credentials and coul ttacks. While these workstations were described as 'legacy' that there is no plan to remove or replace these as has been ther workstations. It is therefore important that the security ient to support the zero trust model which has been adopted.

The white box portion of th oup given more information regarding the setup of the office (suc and their locations, technical details

3 Technical Summary

NCC Group [redacted] Hays to conduct a security assessment of the systems from a position of [redacted] with a view to identify vulnerabilities within the systems in scope in ord[redacted]rity issues that could be used to compromise the network and prolifera[redacted]

Scope

The secu[redacted]t was carried [redacted]ronment (Reading office) and inclu[redacted]ng sections. [redacted]within the scope of each section a[redacted]

- External scanning
  - [redacted]
- Black box/white box internal assessment of Reading office networks including:
  - [redacted](main office (including Corporate Wi-Fi) LAN)
  - [redacted](Management LAN)
  - Wireless networks:
    - Hays_Recruitment_Corp ([redacted])
    - Hays_Recruitment_Guest [redacted])

Caveats

Checks that would have a high probability of causing disruption to the named hosts were excluded. Denial of service attempts were excluded for the same reason.

5 Table of Findings

For each finding, NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors.

Title	Status	ID	Risk
Default [redacted]redentials	New	[redacted]F	High
Default [redacted]s	New	[redacted]J	High
Passwo[redacted]Within the Office	New	[redacted]J	High
Door Ac[redacted]xposed Services	New	[redacted]B	High
NetBIOS[redacted] Enabled	New	[redacted]G	Medium
Weak D[redacted]dentified	New	[redacted]W	Medium
Wireless[redacted]Pre Shared Keys (PSK)	New	[redacted]Q	Medium
Clear Te[redacted]	New	[redacted]W	Medium
Insecure[redacted]dentials	New	[redacted]T	Medium
Weak TL[redacted]	New	[redacted]T	Low
Default [redacted]ng	New	[redacted]X	Low
Poor Ne[redacted]d Hygiene Practices	New	[redacted]E	Info
Closed [redacted]	New	[redacted]B	Info
Only Re[redacted]	New	[redacted]V	Good

6 Risk Ratings

The table below gives a key to the ratings used throughout this report to provide a clear and concise risk scoring system.

It should be stressed [redacted] verall business risk posed by any of the issues found in any test is ou [redacted] means that some risks may be reported as high [redacted] result of other controls unknown to us, be [redacted]

Risk Rating	CVSS Score	Explanation
Critical	9.0 - 10	[redacted] iscovered that has been rated as critical. on as quickly as possible.
High	7.0 - 8.9	[redacted] iscovered that has been rated as high. on in the short term.
Medium	4.0 - 6.9	[redacted] iscovered that has been rated as medium. ved as part of the ongoing security ystem.
Low	1.0 - 3.9	[redacted] iscovered that has been rated as low. This as part of routine maintenance tasks.
Info	0 - 0.9	[redacted] e that is reported for information. This in order to meet leading practice.

16. Table:

Table of this Research Project, where readers can see the ***acronym*** for each word's "***Short-Form***". These are given below:

ISMS	Information Security Management System
InfoSec	Information Security
Cyber Start	Cyber Strategy
G&D	Guidelines and Directions
SOC	Security Operation Centre
NOC	Network Operation Centre
CC	Computacenter
DC	Data Centre
UK&I	The United Kingdom and Ireland
EMEA	Europe Middle-East and Americas (north and south America)
APAC	Asia Pacific
CSM	Cyber Security Manager
ISO	Information Security Officer
GCTO	Group Chief Technical Officer
MS.D	Microsoft Defender
Plug-In SA	Plug-in Security Assessments
WAF	Web Application Firewall
Office 365 (at Hays)	Security Monitoring tool
MS. E5 L	Microsoft E5 License
Tenable SC	Tenable on-premises Vulnerability management solution (Global Scanning Software at Hays)
IRM	Incidents Management and Response
Risk Matrix	Measurement of Risk
Annex	An extra or subordinate part
VA	Vulnerability Assessments
VM	Vulnerability Management
Pen Testing	Penetration Testing
MSP	Manage Service Provider
GDPR	General Data Protection Regulations
CERT	Computer Emergency Response Team
EOL	End of Life Cycle (for software)
EDR	End-Point Detection and Response
CIA	Confidentiality, Integrity, and Availability
SOAR	Security Orchestration, Automation, and Response
IR	Incident Response

17. References:

All references have been provided accurately, where exactly extracted from for this Research Project.

All are included in APA style, and are given below:

[1] Hays Global Cyber and InfoSec Strategy

[2] Hays ISMS Policy

[3] Hays ISMS Lifecycle

[4] Hays SOC Policy

Alongside this, for this Research Project other references are included because Hays is receiving service from the world's largest Tech giants, all are given below:

Microsoft:

[5] Microsoft Defender or MS Defender

[6] Office 365

[7] Microsoft E5 suite or MS E5 License

(2022). Retrieved 31 July 2022, from https://www.microsoft.com/en-gb/

Splunk:

[8] **Splunk Service provider itself**

[9] **Pro-Active monitoring of Hays's Asset by Splunk**

Splunk | The Data Platform for the Hybrid World. (2022). Retrieved 31 July 2022, from https://www.splunk.com/

Tenable:

[10] Tenable SC or Tenable SC (Nessus) Vulnerability Scanning Software

Tenable®. 2022. *Tenable® - The Exposure Management Company*. [online] Available at: <https://www.tenable.com/> [Accessed 31 July 2022].

Furthermore:

[11] 3rd Party Risk Advisory

Riskrecon.com. 2022. *Home | RiskRecon*. [online] Available at: <https://www.riskrecon.com/?hsLang=en> [Accessed 31 July 2022].

[12] Web Application Firewall monitoring (WAF)

Imperva. 2022. *Cyber Security Leader | Imperva, Inc.*. [online] Available at: <https://www.imperva.com/?utm_source=google&utm_medium=cpc&utm_campaign=sw-waf-uk> [Accessed 31 July 2022].

[13] Browsing Plug-in Security Assessments (Plug-In SA)

[14] Hays's Incident Response Management (IRM)

Audit Trail at Hays:

[15] Internal Audit trail – By Hays ISMS team

[16] External by PWC and KPMG

PWC – 2022. [online] Available at: <https://www.pwc.com/> [Accessed 31 July 2022].

KPMG - 2022. [online] Available at: <https://home.kpmg/xx/en/home.html> [Accessed 31 July 2022].

Vulnerability Scanning at Hays:

[17] Internal VA Scanning – A&O IT Group

A&O IT Group. 2022. *A&O IT Group | Global IT Support Services*. [online] Available at: <https://www.aoitgroup.com/> [Accessed 31 July 2022].

[18] External VA Scanning – NCC Group

Softwareresilience.nccgroup.com. 2022. [online] Available at: <https://softwareresilience.nccgroup.com/> [Accessed 31 July 2022].

Penetration Testing:

[19] Pen Testing – NCC Group

Softwareresilience.nccgroup.com. 2022. [online] Available at: <https://softwareresilience.nccgroup.com/> [Accessed 31 July 2022].

The framework used for Hays Cyber and Information Security by the ISMS team:

[20] ISO 27001

[21] ISO27002

[22] ISO 31000

[23] HAYs GAP Analysis materials

ISO. 2022. *International Organization for Standardization*. [online] Available at: <https://www.iso.org/home.html> [Accessed 31 July 2022].

[24] NIST – 800 Family

[25] NIST 800 -53 Access Control

[26] Hays Conditional Access (CA)

NIST. 2022. *National Institute of Standards and Technology | NIST*. [online] Available at: <https://www.nist.gov/> [Accessed 31 July 2022].

[27] **Paragraph number 2 (Scope) in this Research project**:

[This paragraph is a copy of my own work, which I uploaded on my GitHub profile, as it is in progress on GitHub, GitHub. 2022. GitHub - AkmHasan/-: This Research Project will focus to conduct and complete a research based on Hays technologies and its central IT department. It is a global position, as Hays has branches in 23 countries. [online] Available at: <https://github.com/AkmHasan/-> [Accessed 31 July 2022].